技术+法律：区块链时代个人信息权的法律保护

■陈奇伟　聂琳峰

区块链技术填补了传统数据信息时代对个人信息保护的诸多不足，其去中心化特征、公开透明机制以及非对称密码技术能极大程度提高个人信息保护水准。但是新兴技术并不总是完美的，区块链技术也同样如此，其技术本身存在的不可篡改性、匿名性、去中心化等特性在一定程度上与当前个人信息的控制权、删改权、同意权等权属存在冲突，还与传统的监管方式和救济措施存在冲突。要化解这些冲突，应坚持技术服务法律、法律推动技术的基本原则加具体规范的模式，最终实现技术与法律的完美结合，促进技术进步，完善区块链独特内生结构的法律制度，为区块链时代的个人信息权提供法律保护。

[关键词]区块链；个人信息；个人信息权；技术风险

[中图分类号]D922.16　[文献标识码]A　[文章编号]1004-518X(2020)06-0166-10

[基金项目]江西省高校人文社会科学重点研究基地招标项目“大数据时代个人信息权保护的立法问题研究”(JD170096)

陈奇伟，南昌大学立法研究中心研究员、法学院教授。(江西南昌　330031)

聂琳峰，南昌大学法学院硕士生。(江西南昌　330031)

随着互联网的蓬勃发展，数据信息模式进入了新时代，信息存储由硬件储备转为云端备份，极大地推动了互联网经济的发展。但由于互联网的高度开放性，导致了信息安全问题时常发生。2018年，我国发生了包括十几亿条用户快递信息、2.4亿条某连锁酒店入住信息等数据泄露事件，这些数据包含了大量个人隐私信息，给我国广大网民人身、财产安全带来了隐患，致使个人信息遭受严重损害。[1]以上风险超越了传统个人信息保护机制的应对能力。

而区块链的出现恰好可以弥补传统信息储备模式的不足。区块链是一种互联网数据库技术，其采用技术背书的方式，承担了“上帝”的角色。其最显著的特征是去中心化及公开透明，采用非对称密码机制，安全性能极高，可有效保护个人信息。2016年，国务院印发了《“十三五”国家信息化规划》，将区块链纳入新技术范畴并作了前沿布局，这标志着党中央、国务院开始着力推动区块链技术的发展。2019年10月24日，中央政治局就区块链技术发展现状和趋势进行第十八次集体学习，习近平总书记指

出我们应当将区块链作为核心技术自主创新的关键突破口，这一重要论断标志着区块链技术的发展迈上了新台阶。[2]中央的高度重视，为区块链技术的发展营造了良好的政策环境。

不过当下区块链技术并不成熟，在保护个人信息权时也伴随着潜在的风险。如何权衡鼓励技术创新和保护个人信息权两者关系，已成为当下最大的公共政策和法律难题之一。因此，有必要从防范技术风险和完善配套制度建设两方面进行探索，为区块链技术的落地推广保驾护航。

一、区块链技术与个人信息权保护

“我们可能即将迎来一个新革命。”[3]作为比特币的底层技术，区块链技术在过往的数年中渐有星火燎原之势，随着区块链应用场景的不断拓展，社会运行方式也将因此改变。基于区块链技术本身特性，可以预见在个人信息保护领域，区块链将彻底颠覆传统的保护模式。因此，明确区块链技术和个人信息权的内涵和外延，是研究的逻辑起点。

（一）个人信息及个人信息权

根据《中华人民共和国民法典》第1034条的规定，个人信息是指“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、电子邮箱地址、行踪信息等”，其本质属性为可识别性。根据国内通说，个人信息权指的是在收集、处理及使用个人信息的过程中，信息主体享有的知情权和决定权，等同于国外的个人信息自决权。[4][5][6]根据《民法典》第1046条，个人信息权具体包括查阅权、抄录权、复制权、异议权、请求更正权、请求删除权等。根据2016年欧盟颁布的《通用数据保护条例》第3条，个人信息权还应包括控制权、遗忘权、救济权等。[7]按照民法典编撰体例安排，个人信息权编排在第四编人格权中，根据体系解释，应将个人信息权定性为人身权利，可识别性决定了人格属性为个人信息的本质特征。

（二）区块链技术的特点

区块链是一种依照时间排序将数据区块以链状方式组合形成的特定数据结构，并以密码学方式保证其不可篡改和不可伪造的去中心化、去信任的分布式共享总账系统。[8]区块链具有以下几项关键技术：（1）以时间戳为基础的链状结构。区块链可分为“区块+链”，其中“区块”又可分为“区块头+区块体”，“区块”都有唯一的哈希值与之对应，本区块头记录上一区块的哈希值，本区块体存储数据信息。同时，每个区块生成时都会加盖时间戳，随着时间的延长，形成了拥有时间维度的链条，保证了信息的可追溯性。简单来说，就好比将区块比作A4纸，将链比作A4纸的页码，通过先后顺序排列从而形成完整的区块链。（2）以P2P为基础的数据传输系统。区块链以P2P分布式网络架构为基础，运用互联网传输信息，网络中每个节点地位相同，不存在核心节点，实现了去中心化。同时每个节点都充当路由器，将上游区块传输的信息向下游区块传递，并且具备验证功能，只有经过所有区块认可的信息才可上链，保证了信息的不可篡改性。（3）分布式节点共识机制。共识机制的目的在于根据事先协商一致的规则使各节点对交易信息达成共识，保障了信息的一致性、真实性。（4）智能合约。智能合约是基于预定时间触发、不可篡改、自动执行的程序，是由代码构建的多方承诺。合约签订前，合约所有内容已经制定好，当事人之间不用达成合意，而是依靠技术背书进行可信数据交互，系统会自动撮合、自动执行，不存在违约可能性。

（三）区块链在个人信息权保护方面具有的优势

区块链通过加密算法、P2P网络、共识算法等互联网技术，为参与者提供了可信、透明的商业

处理逻辑框架,其技术结构使得区块链在个人信息权保护方面具备如下优势。

去中心化。区块链上数据的验证、存储、维护和传输等均是基于分布式系统结构,利用算法来构建分布式节点之间的信任关系,从而形成非中心化的分布式系统[9],其不存在中心化设备和管理机构,各节点地位平等,部分节点的损坏不会对区块链整体产生影响,保障信息的安全存储。在传统中心化信息管理系统中,一旦攻击者入侵中心节点,将会导致整个系统陷入崩溃[10],甚至可能有中心信息机构主动出卖用户信息以谋取私利,而在去中心化的框架下,将难以出现以上问题。

不可篡改性。对上链信息附上时间戳,之后下游区块的时间戳都会对前一个时间戳进行增强,通过时间戳的前后延续确保信息不被篡改。[11]若要修改本区块信息,还需要改变其他所有区块信息,并经过共识机制的认可,除非能够同时控制系统中51%以上的节点,否则难以实现。在传统中心化网络模式中,外部攻击者或者内部工作人员很容易就能够侵入信息系统,进行数据篡改、删除等非法行为。

开放性和可追溯性。区块链系统是透明的,除了各自的私有信息被加密外,其他所有信息对所有参与者开放,任何单一节点都可以获得其他节点所有的数据信息。同时,因为区块链是依据时间先后顺序记录信息,所以保证了用户能够对信息进行追溯调查,从而保障个人信息权中的查询权、抄录权、复制权。在传统信息数据库中,各中心信息平台存在较为严重的信息孤岛现象,平台之间信息隔阂,信息碎片化严重,只具备局部开放性,同时信息整合混乱,难以追溯有效信息。

匿名性。由于各节点之间无须相互信任,因此无须公开身份,整个交易过程中,交易双方仅仅知悉交易对象的公钥地址,其实际身份无从知晓,进一步保障了参与方的隐私权。[12]

便于监管,减少风险。区块链能够存储、保留所有信息,而且区块链透明、可追溯、不可更改,有利于监管者追溯、核查、验证信息。传统中心系统一旦遭遇故障或攻击,会造成系统整体瘫痪,而区块链依靠分布式节点存储信息,部分故障不影响整体,每个节点均包括区块链信息副本,容错度高,可减少系统性风险。

二、区块链技术给个人信息安全带来的挑战

虽然区块链技术在保护个人信息权方面具备诸多优势,但由于技术本身不够成熟,区块链仍然面临着巨大的安全威胁,这也是区块链技术具体运用于信息安全领域时必须要解决的核心问题。

(一)不可篡改性与个人信息更正权、被遗忘权之间存在冲突

更正权是指当信息权利人认为信息存储机构所记载的个人信息存在不准确、不完整的情形时,可以请求存储机构予以更正的权利。被遗忘权是指当出现约定或法定事由时,信息主体有权要求信息管理方销毁信息,其他机构及个人不得援引或使用。[13]

当前的区块链技术以平台式运用为主,已有的中心信息库与链上信息之间不存在必然关系,区块链技术只能保证链上所有节点之间信息的一致性,而无法确保上链数据本身是否真实可靠,因此区块链技术无法避免信息自身存在的瑕疵。[14](1)信息内容自身可能有误。区块链作为底层技术,主要保证的是信息交换效率最大化和信息之间一致性,而无法确保上链前信息的真实性。(2)信息共享可能发生错误。即使信息本身属实,但人员或设备可能在导入过程中发生错误,例如不熟悉操作流程的过失错误或者存在个人非法企图的故意错误,都会导致信息不真实。(3)链上信息只可增加不可删除,那么用户身份信息、账户信息、证书信息及其他个人信息的更新和撤销就成为问题。(4)一旦用户不小心将隐私信息、敏感信息等不应公开的信息传至链上,将会导致权

利人陷入无法挽回的境地。

因此,区块链技术的不可篡改性与更正权、被遗忘权存在冲突,那么如何实现技术与法律相互融合就成为当下的难题。

(二)匿名性与个人信息控制权、同意权之间存在冲突

根据《中华人民共和国民法典》第1035条的规定,控制权是指信息主体对个人信息享有占有、使用、收益及处分的权限,不受任何其他限制;同意权是指当他人收集、处理权利主体个人信息时,须经权利主体同意。传统的身份账户由第三方维护,当账户信息意外丢失时,用户可以凭借有效身份证明重置账号密码予以找回。区块链采用的是非对称密码技术,保证链上特定信息资产对应特定权利主体。公钥即身份,或称之为"账号",里面包含着个人信息资产,私钥即"密码",私钥仅为权利主体所知晓,在现有算法技术下,通过全网公开的公钥反向破解私钥几无可能,具备极强的匿名性,只有当私钥与公钥验证一致时,个人信息所有人才能维护链上信息资产。[15]因此,权利人对私钥的管理直接关系到个人信息控制权、同意权,当权利人对私钥管理不当时容易与区块链的匿名性之间产生冲突。

一是权利主体私钥丢失难以找回。根据区块链技术本身特性,权利人只能通过私钥管理自身信息,从而确保绝对的安全性。一旦私钥遗失,依靠目前已有算力很难反推私钥,权利人将对个人信息彻底丧失控制。[16]

二是匿名性导致无法判断私钥使用者是否为本人。基于私钥的唯一性,恶意第三人在链上可能难以对权利主体的信息实施攻击,不过其可以通过其他方式获取私钥,从而掌控权利主体的信息,实施严重损害个人信息权的行为。比如,用户可能将私钥储存在链下电子设备中,相当于将私钥托付给第三方可信机构,这违背了区块链去中心化的初衷,那么黑客可能以电子设备作为攻击目标,进而窃取私钥;或者通过借用合同获取私钥后,超出约定使用范围,侵害个人信息权。

三是匿名性导致用户相对性,难以保护信息控制权。[17](1)区块链完全透明,其存储的交易信息直接暴露在区块链中,任何人都可以获得。通过利用数据挖掘、分析技术,可以发现地址之间、交易之间的相关关系,从而推测用户身份。例如,从交易入手,根据交易实际价值,搜索与交易相关的有效地址,再根据活跃度和地址之间的关联,筛选出有效用户信息,进而推测出用户真实身份,获取私人信息。[18](2)虽然区块链系统具备极强的安全性能,篡改链上信息须达到51%攻击才行,即控制半数以上节点。但随着技术的不断进步,区块链也可能被攻破,例如量子计算机的算力能够破解目前最强电脑都难以破解的加密算法,当达到51%控制之后,黑客便可随意修改链上信息,这将导致不可估量的损失。

(三)去中心化与传统监管模式之间存在冲突

现在主流的信息管理模式都是以政府或者信息存储中心为核心, 比如个人不动产信息须经有关房管部门登记,银行账户信息须由银行等金融机构审查确认。由此可见,当前存储模式与监管模式很好地实现了"技术+法律"的统一,存储采取中心储备模式,监管相应采用了中心监管模式,政府部门或者相关信息存储机构就是监管核心。针对传统监管模式,我国出台了诸多法律规范,如《网络安全法》第31条规定,信息基础设施运营商应当履行法律规定的信息安全保护义务,设置专门安全管理机构和安全管理负责人;又如《信息安全等级保护管理办法》《征信机构信息安全规范》中对信息系统和服务器的安全等级要求、地理位置要求的规定均是中心化的。

然而,区块链技术去中心化的理念与现有法规要求和中心管理思想背道而驰,区块链技术环环相扣,外部监管措施很可能牵一发动全身。(1)传统监管手段在保护链上个人信息权时监管不

力。其一,对技术本身无法有效实施监管;其二,对链上信息难以实施有效监管,链上信息散落于各个区块参与者手中,不再集中于中心管理机构,传统监管缺少监管的抓手,若需要实施有效监管,将被迫扩大监管范围,监管力量将被分散、弱化,这将极大程度增加监管难度;其三,去中心化导致被监管主体不明确,例如没有典型的内部组织架构和实体,监管难以落地。[19](2)监管制度存在滞后性,区块链相关管理制度空白。区块链创新是由技术引导的,但监管和立法相对滞后,可能会导致市场主体抓住创新和监管跟进的间隙肆意妄为,引发混乱。不过对于区块链技术相关立法已经开始逐步展开,国家互联网信息办公室(以下简称网信办)颁布了《区块链信息服务管理规定》(以下简称《区块链规定》)并于2019年2月15日施行,其中规定了信息服务提供者的相关责任,并明确各级网信办负责本区域内的区块链信息服务监管工作。然而此规定仅有24条,内容宽泛模糊,对技术特性与监管性质存在的冲突只字未提,难以应付具体运用场景中的突发情况。

(四)救济途径、责任主体与个人信息救济权之间存在冲突

依据传统法律规范,当个人权利遭受损害时,可以通过诉讼、仲裁、调解等方式请求侵权方承担刑事、行政或者民事责任。随着区块链科技的迅速发展,现有法律框架已难以适应新科技的冲击,现有规范难以涵盖和调整新的权利义务形态,个人信息权遭受侵害时,认定法律责任归属和提供信息权利救济面临障碍。(1)明确责任主体是承担责任的首要前提。区块链自身具备匿名性和开放流动性,各节点实际上已人格化,但节点人格与现实法律人格并非一一对应,因此即使产生信息侵权事实,也难以确定背后侵权主体。[20](2)当区块链系统遭遇黑客攻击或者系统运行错误导致大量信息数据泄露时,很难在开源软件编程者、系统运营参与者、系统操作使用者、第三方应用或服务提供者等主体之间识别并认定适格的责任主体。(3) 即便能够识别并认定具体主体,根据我国目前有关区块链的规范,仅规定了区块链服务提供者的义务,对如何救济使用者权益未置可否。究其原因,一方面没有明确归责原则,严格责任不利于技术发展,过错责任难以认定主观动机,行为与结果之间的因果关系的认定也存在巨大阻碍;另一方面很难明确责任的具体承担方式,例如基于技术的不可逆转性,除非51%的节点同意放弃本区块,否则针对个人信息遭受侵害的事实,被侵权人只能请求事后补偿,技术上无法恢复原状。

三、区块链时代个人信息权保护的对策

鉴于区块链技术与现行个人信息权保护法律制度之间的冲突,若处理得当,就可以破解零和博弈的难题。解决难题应明确的基本原则是:技术服务法律,法律推动技术。(1)技术应当为法律服务。区块链是一种通用型技术,在征信、保险、金融、司法存证等领域都有所运用,理论上,也可以为法律体系所借鉴,使之成为维护法律规范、保障法律运行的工具。例如,可以利用技术代码确保监管对象遵守法律,降低执法成本,该类科技被称为“监管科技”①。以R3联盟的Corda项目为代表,其运行旨在执行法律条文或约定协议,美国伊利诺伊州是第一个正式加入R3联盟的政府机构。[21](2)法律理应推动技术发展。纵观人类社会进程,每一次社会大进步都是由科技率先推动的,面对新技术,法律制度总是滞后的,对于新生事物,我们应当给予其一定的制度环境和成长空间。[22]区块链发展之所以如此迅速,正因为其能够提高交易效率、保障交易安全、维护个人信息。当然,过度强调“技术中立”也不正确[23],技术并非独立于规范之外,技术的运用总是被赋予了价值偏好,由人类控制的技术难以实现真正的技术中立,由技术引发的风险正是法律介入的逻辑起点。古人云:“没有规矩,不成方圆”,法律规制是区块链技术发展的必由之路。

因此,我们应该平衡技术创新和法律规制的关系,促其良性互动与融合。在价值维度上,在支持区块链技术创新的同时保持审慎姿态,为新技术运用设定不违背法律基本原则的整体框架,纠正不符合法律核心价值的技术偏好;在规范维度上,将技术规范纳入法律制度范畴,建立技术与法律相融合的法律体系,同时保持谦抑性,防止法律过于严苛阻碍技术进步,明确法律约束的范围及程序,为区块链发展提供良好的法治环境。[24]具体对策建议如下。

(一)为更正权、被遗忘权的实现提供完备渠道

法律之所以设定更正权、被遗忘权,主要目的在于避免错误信息或过时信息在信息交换中妨碍权利人正当行使信息权,比如征信机构可能调用个人错误信息作为信用评价基础。所以,我们可以从法律目的出发,从技术和制度层面构思如何化解冲突。

1.为更正权提供救济渠道。假如权利人某项信息确有错误,可以将更正后的数据上传至链上,上传过程同样需要遵守区块链一般规定,须经所有节点一致认可,防止权利人擅自上传信息,保证区块链系统的稳定性、可预见性。同时,基于时间戳技术,链上信息不可篡改,更正前后的信息均按照时间顺序储存在链上,可以在更正前后的信息上都附上超链接,当他人运用权利人个人信息时,对于前后不一致的信息可以根据时效原则进行取舍。不过,此方式同样存在弊病,因为区块链系统存在延时效应,须经其他区块认可以后才可上传更正信息,可能因为时间差会导致部分纠纷。针对隐私信息、敏感信息等,可以利用智能合约,设定前置自动化审查程序,对于带有敏感词、敏感代码等信息,合约自动不执行上传程序,原路退回用户或存至链下数据库。

2.为被遗忘权提供救济途径。被遗忘权是针对过时信息而言,主要体现在征信领域,防止过时信息让征信机构产生信赖,从而影响权利人实现自身权利。技术上我们无法删除过时信息,但是可以在智能合约中设定信息使用有效时限,通常为5年,当征信机构使用5年前个人信息作为信用评价基础时,权利人可以向征信机构反映、投诉等,甚至以违反智能合约为由追究对方违约责任。征信机构确需使用5年前信息的,须经权利人同意并且履行使用说明义务。通过智能合约合同法保护,有利于权利人等同实现被遗忘权。[25]

(二)为控制权、同意权的实现提供完善途径

针对新技术引发的法律风险,可以采取“技术+法律”双层保护模式。在技术层面,尽量完善技术,防范技术风险;在制度层面,宏观上完善配套法律制度,微观上更新监管方式。

1.私钥实体化,提高权利人私钥管理能力。一是增强权利主体私钥保护意识,提示私钥管理重要性;二是将原本电子化的私钥实体化,将内容记入脑海中,同时将私钥放置于保险柜中并实施备份,避免遗失。若权利人确实遗失的,可以由市场提供保险等新型风险管理产品,针对系统风险与非系统风险设定不同的保险额,区块链金融对此已有所涉及。安全措施是否充分,与个人信息对个人的影响呈正相关系,对个人利益影响大的敏感信息,需要采取更充分的保障措施。[26]

2.增加身份认证技术,防范他人恶意使用私钥。可以在区块链技术基础上,添加身份认证技术,例如通过用户口令、数据证书、身份证件和生物表征(如声音、指纹和虹膜等)来确认用户真实身份,将私钥的使用与个人身份信息结合。同时,为了防止身份认证信息被黑客篡改,可以利用区块链分布式账本记录身份认证信息并生成用户证书,将用户证书与公钥相对应。只有当代表身份认证信息的私钥与代表用户证书的公钥对应一致时,才能操作账号。

3.链上链下结合,摆脱匿名性导致的用户相对性。(1)大部分区块链系统完全透明,未能对个人信息进行加密保护。对此,笔者建议采用链上链下结合保护的模式,将数据管理与数据存储相分离,将数据索引和操作权限交由区块链处理,将真实信息存储于链下数据库中,链上信息共享

时,仅共享信息的地址,不共享信息的内容。(2)针对未来可能出现的51%攻击导致区块链系统性破坏的行为。一是增强哈希值的复杂程度,研究可以抵抗量子计算攻击的密码学算法;二是建立完善的防火墙制度,对异常链接立即自动拦截;三是对操作异常的节点设定访问权限,提高准入门槛;四是强化代码安全审计,及时发现代码缺陷。

4.制度层面制定风险应对策略。(1)出台对应安全标准和管理规范。当前我国已有部分相关规范,例如2018年工信部正式颁布《区块链和分布式账本技术参考框架》,不过该文件未能涵盖区块链应用的所有领域,应当继续由有关部门出台管理条例和应用指南,同时鼓励社会力量展开区块链安全标准细化工作,如建立准入资格审核制度、落实安全负责人职责、实行网络安全监测预警制度、健全信息通报制度、展开风险评估工作,并定期组织风险应对演习,在事前形成第一道风险屏障。[27](2)建立风险紧急处理预案制度。根据事件危害程度划分等级,规定对应处置措施,一旦突发风险,立即启动风险处理机制,如发布公告、临时限流、紧急关闭、启动黑名单、系统整改、约谈安全负责人等,防止事态扩大化,将损失最小化,在事中形成第二道风险屏障。

(三)完善配套监管措施,建立行业自律机制

由于区块链去中心化的技术特点与传统法律监管方式完全背离,去中心化的优势在于单点故障不会引发系统故障,但对于监管而言则并非善事,因为若要对区块链进行干预,须以整个区块链系统为对象,难以追究单个主体的责任。[28]不过,网络家长主义者认为,网络空间仍处于法律规制范围之内。如Lessig指出,政府能够在网络中设定代码对网络空间实施监管。②De Filippi主张,监管主体可以将区块链作为监管手段,从而提高监管效率、扩大监管范围。事实证明,虽然网络空间虚无缥缈,但是网络服务机构、人员却是真实存在的,所以网络和监管并不冲突。[29]

1.改变传统监管手段,提高监管效率。(1)可以借鉴De Filippi的主张,利用区块链去中心化的特征,将监管者放置到区块链中,使之成为其中一个"监管节点",这有利于监管机关实时监控并全盘掌握所有信息,及时发现链上问题并加以处理。甚至,监管机关可以成为"超级节点""多中心节点",只要掌握了足够的算力,就能掌握更多数量的区块,从而在制定链上公约时增加其话语权。监管机关可以将链上公约规范化,形成链上法则,对上链、运行、下链、惩罚等制定规范,并使其代码化,成为智能合约,成为区块链运行一部分,最终建立监管机制,实现技术+法律相融合。[30]根据《区块链规定》,网信办为区块链监管机关,区块链信息服务提供者为区块链中重要节点,信息服务提供者应制定管理规则和平台公约。这与前文论述刚好相符,体现了传统中心治理思维向"以链治链""法链"治理思维的转变。[31](2)实行各节点差异化信息提供标准。在节点初始加入区块链时,仅要求提供最低限度的信息,当节点行为一直保持正常,信息提供维持最低标准,一旦节点出现异常举动,根据异常程度、算力等级,强制要求节点提供相应个人信息,这为监管提供了方向和抓手,有利于维护信息安全。

2.细化区块链监管制度,扩大监管范围。我国已制定《区块链规定》,但其内容过于笼统模糊,无法有效解决现实难题。对此,建议加快立法进程,出台更多可以落地的操作规范和使用指南,提高监管适应性,在法律规范调整范围之内引导区块链技术发展。具体举措可以参考美国和英国相关规定。(1)在监管对象上,美国分为两类:一是区块链平台及服务提供商,其数量少但地位重要,是核心监管对象,应当审查其忠实义务和勤勉义务履行情况;二是区块链用户,其数量众多但价值密度低,往往不对其进行过多监管,享有豁免权。(2)在备案登记上,美国在FinCEN监管指南中规定,区块链平台和服务提供商等必须履行备案手续,明示承担反洗钱义务和识别用户身份义务,以便事后政府调用信息和追究问责。(3)英国创新性地提出了"沙盒监管",在试点取得良好效

果后,于2016年正式推广。其内容为:由政府根据企业规模和用户福利,筛选申请沙盒监管的企业,同时政府会选取部分消费者体验企业内测平台,如果效果达到预定目标,申请企业可以将内测平台向社会推广,之后政府仍会根据用户报告和测验结果不断调整监管措施。[③]我国江西赣州和贵州已有部分实践,这为我们今后推广沙盒监管提供了宝贵的经验。(4)2017年上海市互联网金融行业协会发布了《互联网金融从业机构区块链技术应用自律规则》,其中第4条要求从业机构在向社会公开区块链产品时,应当通过第三方评估、测试,获取律师出具的法律意见书,同时做好信息披露工作,第6条规定区块链产品不得利用技术特点排除法律适用,同时应当通过风险管控与合规评估,这与沙盒监管一脉相承,有利于实现监管下的技术创新。[32]

3.应当在政府部门的指导下,完善行业自律机制,促使行业协会成为有效的第三方监管机构,具体落实监管工作。[33]例如,采用多中心治理模式,行业协会也作为中心节点加入区块链,对于个人信息保护运行全程监控;制定统一的区块链技术标准,主导区块链技术话语权;开展国际交流与合作,学习先进经验,建立多边区块链治理体系;制定链上行业公约,促使个人信息保护规范化;开展区块链安全教育工作,培养安全人才;鼓励个人信息保护技术创新,对优秀技术提供者发放奖励;定期对节点进行评级,公示评级结果;对个人信息保护合规的节点,颁发认证证书。最重要的是,应建立链下个人信息保护申诉、投诉制度,设立申诉、投诉机构并制定处理流程。[34]

(四)提供有效救济途径,明确法律责任内容

《区块链规定》明确网信办是区块链信息服务监管执法机构,规定信息服务提供者承担信息内容安全管理责任,并规定了信息服务提供者在违反本规定时应承担的行政责任、刑事责任。但其涉及面狭窄,内容笼统,难以应对复杂多变的实际状况,应当更加精细化,增强可操作性。

1.明确责任主体和归责原则。(1)区块链系统遭遇黑客攻击时,因为黑客攻击属于性质恶劣的故意行为,应当将黑客作为责任主体,可按照刑法进行严厉惩处;(2)对信息服务提供平台,应强化其安全管理人责任,设置安全保障义务,并设定惩罚性损害赔偿,适用过错推定原则;(3)对系统开发人员的原因导致的损害,因为系统开发错误属于系统性漏洞,影响范围较广,应当施加定期审计义务,按照过错推定原则予以追责;(4)对系统服务人员和运营人员,可以采取过错责任原则;(5)对主管机关监管不力的行为,可以通过行政复议、诉讼、控告等方式,请求履行行政义务、承担行政责任;(6)对信息主体操作不当导致的自身损失,可以按照公平责任原则由平台适当补偿;(7)兜底条款对于其他任何侵犯个人信息权的行为,根据不同法律规范,依据责任程度大小,请求对方承担相应责任。总之,应制定责任分配机制,实行责任限额制度,保护个人信息权。

2.以民事责任为主的责任承担方式。(1)停止侵害、排除妨害。对于作为侵害行为,权利人可以请求对方停止侵害,对于不作为的侵害行为,可以请求对方排除妨害。(2)消除影响、恢复名誉。对于侵权人不当公开个人信息,导致权利人社会评价因此降低的,侵权人应当采取适当方式消除不利影响,恢复权利人社会声誉。(3)赔礼道歉。基于个人信息权的人身权属性,权利人可以请求对方赔礼道歉。(4)返还财产。对于侵权行为导致的财产性损失,能够返还的应当立即返还。(5)赔偿损失。对于财产性损失,不能返还的应当赔偿等同于财产价值的金额,对于人身性损害,往往不方便直接用金钱衡量,赔偿数额可以根据侵权人因侵权行为所获取的收益来确定。具体履行上述金钱给付义务时,可以利用智能合约自动执行功能,根据智能合约应用程序端口接收的物联网传导器数据,自动从侵权人处划转对应金额至受害人账户。

3.其他法律救济建议。(1)针对区块链时代个人信息权被大范围收集和处理的情形。对于侵权人而言,他们的行为对整个区域都会有较大损害;对权利主体而言,仅是个人信息权的轻微损

害。因此,可以采取公益诉讼、集团诉讼、小额诉讼等模式来处理纠纷,也可以通过网上仲裁、调解等方式化解矛盾,最后通过智能合约自动执行民事责任内容。(2)合理分配举证责任。权利人和侵权人一般处于信息、资源不对等的地位,因此在个人信息权侵权诉讼中,可以采取举证责任倒置方式,让侵权人对其履行了安全保障义务或收集、使用、管理个人信息的合法性提供证明。(3)明确司法管辖权。基于区块链的匿名性和非实体性,可以参考下列管辖权确定规则。优先根据当事人意思自治确定管辖权;未达成合意的,根据链上记录信息、当事人住所地等来确定;如果按照个人信息无法判断管辖地的,可按照平台所在地确定;鼓励建立线上争议解决机制,这顺应了区块链的发展潮流,提高了纠纷处理效率,我国《电子商务法》第63条亦体现了这一趋势。

四、结 语

区块链技术对个人信息保护既有技术优势,也存在明显的制度冲突。如何防范技术风险和完善配套法律制度,既要处理好技术创新和法律规制两者关系,又要结合区块链独特的内生结构提出针对性法律对策。正如古人云:"立治有体,施治有序。"[35]未来,我国应当继续深化对区块链技术和个人信息法律制度的研究,以技术+法律双层保护为原则,及时回应立法需求,突破立法和技术难关。

注释:

①The UK's Cheif Scientific Adviser refers 'RegTech' as encompassing 'any technological innovation that can be applied to or used in regulation, typically to improve efficiency and transparency' Government Office for Science (2015) Fintech Future: The UK as a World Leader in Financial Technologies. London.47.

②See Wu T. and Goldsmith(2008).

③See FCA.Regulatory Sandbox.

[参考文献]

[1]国家计算机网络应急技术处理协调中心.2018年我国互联网网络安全态势综述[R].2019.

[2]中国信息通信研究院.区块链白皮书(2019)[R].2019.

[3]Melanie Swan. *Blockchain:Blueprint for A New Economy*,vii,Tim McGovern et al. ed.2015.

[4]吕炳斌.个人信息权作为民事权利之证成:以知识产权为参考[J].中国法学,2019,(4).

[5]洪玮铭,姜战军.社会系统论视域下个人信息权及其类型化[J].江西社会科学,2019,(8).

[6]王利明.论个人信息权的法律保护——以个人信息权与隐私权的界分为中心[J].现代法学,2013,(4).

[7]刘敖迪,杜学绘,王娜.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).

[8]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研究报告[R].2018.

[9]Swanson T. (2014)*Great Chain of Numbers*[EB/OL].Creative Commons, http://www.ofnumbers.com /the-guide/.

[10]孙国梓,王纪涛,谷宇.区块链技术安全威胁分析[J].南京邮电大学学报(自然科学版),

2019,(5).

[11]郑戈.区块链与未来法治[J].东方法学,2018,(3).

[12]杨东.链金有法——区块链商业实践与法律指南[M].北京:北京航空航天大学出版社,2017.

[13]齐爱民.中华人民共和国个人信息保护法示范法草案学者建议稿[J].河北法学,2019,(1).

[14]石超.区块链技术的信任制造及其应用的治理逻辑[J].东方法学,2020,(1).

[15](美)Narayann A., Bonneau J., Felten E., Miller A., Goldfeder S.区块链技术驱动金融:数字货币与智能合约技术[M].林华,王勇,译.北京:中信出版集团,2016.

[16]解黎,姚世坤.区块链技术在征信领域应用探究[J].征信,2018,(8).

[17]Monaco J.V. *Identifying Bitcoin users by transaction behavior.* SPIEDSS, 2015.

[18]任仲文.区块链领导干部读本[M].北京:人民日报出版社,2018.

[19]高兰平.区块链:去中心化恐怕难以监管[EB/OL].http://www.vccoo.com/v/bA4850.

[20]汪青松.区块链系统内部关系的性质界定与规则路径[J].法学,2019,(5).

[21](英)Yeung K.区块链监管:"法律"与"自律"之争[J].林少伟,译.东方法学,2019,(3).

[22]苏宇.区块链治理之现状与思考:探索多维价值的复杂平衡[J].中国法律评论,2018,(6).

[23]郑双玉.破解技术中立难题——法律与科技之关系的法理学再思考[J].华东政法大学学报,2018,(1).

[24]万国华,孙婷.证券区块链金融:市场变革、法律挑战与监管回应[J].法律适用,2018,(23).

[25]李鑫淼."区块链+个人征信"业务的个人信息权保护[J].证券法律评论,2019,(1).

[26]黄武双,谭宇航.机器学习所涉及数据保护合理边界的厘定[J].南昌大学学报(人文社会科学版),2019,(2).

[27]赛迪智库网络空间研究所.我国区块链发展现状、问题、趋势与对策建议[N].中国计算机报,2018-12-17(8).

[28]De Filippi P. & Loveluck B. *The Invisible Polities of Bitcoin: Governance Crisis of a Decentralised Infrastructure*. Internet Policy Review 5(3),2016.

[29]赵磊.区块链如何监管:应用场景和技术标准[J].中国法律评论,2018,(6).

[30](美)Werbach K.信任,但需要验证:论区块链为何需要法律[J].林少伟,译.东方法学,2018,(4).

[31]杨东."共票":区块链治理新维度[J].东方法学,2019,(3).

[32]崔志伟.区块链金融:创新、风险及其法律规制[J].东方法学,2019,(3).

[33]*Madrid: IOSCO analyzes potential of tech-driven change in the securities market industry,* Media Release, 2017-02-08.

[34]陈奇伟,刘倩阳.大数据时代的个人信息权及其法律保护[J].江西社会科学,2017,(9).

[35]谢文.政治建设:立治有体,施治有序[N].光明日报,2018-03-04.

【责任编辑:胡　炜】