

在线平台企业个人信息保护的智能合约机制构建

许娟, 黎浩田

(南京信息工程大学法政学院, 江苏南京, 210044)

摘要: 个人信息保护政策是在线平台企业为维护用户个人信息权益, 根据现行法律法规制定并详细说明其在获取、管理及保护用户个人信息方面的措施及文本。智能合约作为涵盖告知同意规则并自动执行的特定代码程序, 在智能化应用场景下可用于实现个人信息保护政策。进入实施层面的我国《个人信息保护法》需要通过一定的程序机制来保障企业个人信息处理行为合规, 现存程序机制的非智能化难以应对个人信息处理者凭借技术优势造成的过度收集和滥用现象。因此, 有必要尝试运用智能合约的技术性管理功能弥补企业个人信息保护政策的不足, 具体措施为: 将作为智能合约底层技术的区块链进行针对性改造, 使其达到保护个人信息的要求, 进而发挥智能合约个性化拟制和动态化控制特性保障告知同意规则的实现, 将智能合约嵌入在线平台企业处理个人信息的全过程, 构建用户与平台之间以智能合约为核心的个人信息保护政策。

关键词: 智能合约; 在线平台企业; 个人信息保护机制

中图分类号: D923

文献标识码: A

文章编号: 1672-3104(2022)06-0041-14

随着互联网产业盈利模式从在线广告逐渐向基于大数据的定向推送、精准营销转变, 在线平台企业处理用户个人信息的过程出现以“过度收集”和“滥用”为突出特征的乱象。为进一步整治此类个人信息处理违法违规行为, 工信部印发《关于开展信息通信服务感知提升行动的通知》, 要求相关企业建立已收集个人信息清单和与第三方共享个人信息清单的双清单制度^[1]; 此外, 多部门联合印发《App违法违规收集使用个人信息行为认定方法》^[2], 作为认定 App 违法违规收集使用个人信息行为的参考。自此, 以北京微梦创科网络技术有限公司^[3]和北京微播视界科技有限公司^[4]为代表的大型在线平台企业制定了个人信息保护政策, 或在以往的隐私保护政策中大幅增加个人信息保护相关内容。虽然在线平台企业以《信

息收集清单》和《第三方合作清单》为重要组成部分的个人信息保护政策体系逐渐成型, 但由于技术驱动的个人信息处理行为本质上为科技活动, 始终潜藏着对个人信息的泄露与滥用风险, 甚至存在诱发系统性风险的可能。

智能合约作为特定条件达成后自动执行的代码程序是科技治理的一项重要手段, 其动态控制和自动执行等特性使之能够成为悬在个人信息处理者头上的“达摩克利斯之剑”。本文试论述将智能合约作为“双清单制度”实施落地中的技术治理手段, 对我国《个人信息保护法》颁行前在线平台企业普遍形式化的“隐私保护机制”进行程序机制的智能化迭代升级, 以期推动在线平台企业的个人信息保护从以隐私保护机制为标志的形式合规阶段迈向以智能合约程序机制为核心的实质合规阶段。

收稿日期: 2022-03-08; **修回日期:** 2022-08-24

基金项目: 国家社科基金重大项目“构建人类命运共同体国际法治创新研究”(18ZDA153); 国家社科基金一般项目“个人信息权利行使的平衡机制研究”(19BFX127)

作者简介: 许娟, 女, 湖北仙桃人, 法学博士, 南京信息工程大学法政学院教授、大数据法治研究院院长, 主要研究方向: 网络与信息法; 黎浩田, 男, 藏族, 四川甘孜人, 南京信息工程大学法政学院博士研究生, 主要研究方向: 网络与信息法, 联系邮箱: 732199073@qq.com

一、在线平台企业个人信息保护政策的欠缺及其原因

在个人信息处理活动中,个人往往难以知晓其何种信息将以何种方式被处理,也难以了解其个人信息被用于何种处理目的,更难以预测个人信息处理活动可能产生的效果与影响^[5]。在线平台企业个人信息保护政策虽在形式层面已逐渐完成从隐私保护体系时期的单一文本向政策、清单、协议等多个组成部分的体系性文本过渡,但仍存在个人同意失灵、敏感个人信息保护不周等实施层面的问题,其背后的深层次原因是作为程序组合及其运行机理的程序机制未发挥应有作用。我国《个人信息保护法》第11条作为个人信息保护治理的基本原则,不仅在个人信息保护治理主体上将在线平台企业囊括其中,也为通过信息科技构建程序机制实现个人信息权益保护提供了开放接口^[6]。

(一) 在线平台企业个人信息保护政策实施的欠缺

个人信息保护作为数字时代的基础性问题,具有复杂的经济社会面向,也意味着治理措施需要广泛考虑经济社会发展情况、行业特点和社会诉求。在《个人信息保护法》的实施适用中,在线平台企业的应用程序及其分发平台已经成为个人信息保护的关键领域。但由于《个人信息保护法》对损害个人信息的行为大都采用概括性规定,即多数规范尽管设置笼统的个人信息权益保护义务,却并没有明确义务实现的有效路径,由此导致平台所制定的个人信息保护程序机制在实际运行过程中存在如下不足之处。

第一,缺乏贯彻《个人信息保护法》基本原则的有效适用的程序机制。数字经济领域的立法往往带有较多的原则性规范,我国《个人信息保护法》在第一章总则中规定的合法、正当、必要和诚信原则,目的限制与最小化原则,公开透明原则与责任原则等分别表达了处理个人信息应当遵循的基本要求^①。尽管现行法给予了个人信息保护以法律依据,填补了长期无专门立法的空

缺,然而这种原则性规定由于缺乏有效适用的程序机制,陷入被动规制与事后救济的泥淖之中。譬如,第5条涉及的正当原则要求手段正当,但部分在线平台企业作为个人信息处理者通常利用用户画像,锁定特殊消费群体,实施价格歧视、价格混淆等销售策略,导致会员用户支付的价格反而比普通用户更高。例如,在胡某诉上海携程商务有限公司侵权纠纷一案中,携程公司通过算法对用户采取大数据杀熟,实施不合理的差别待遇^[7]。针对实践中不断涌现的大数据杀熟,亟须通过自动化手段予以及时矫正,更新底层技术逻辑,以构建个人信息保护政策的程序机制。此外,必要原则要求个人信息处理者的个人信息处理行为不超过必要限度,其处理个人信息应当限于满足处理目的的最小范围之内,但在线平台企业中普遍存在非法获取个人信息、超范围收集个人信息、过度索取权限等现象。对个人信息处理者的行为缺乏明晰的最小目的认定机制,导致以企业利益为导向的程序机制难以提高事前对风险的可预见性,也未能避免监管部门事后对在线平台企业的随意追责。究其原因,在于没有内嵌技术实现自动化与精准化执行的程序机制,陷入“按需求处罚”或“运动式执法”的境地,因而亟须纾解脱离法治框架的技术风险。

第二,欠缺贯彻同意规则的程序机制,难以解决《个人信息保护法》实施中的同意失灵及其透明度问题。我国《个人信息保护法》涉及“同意”的13个条款主要聚焦于提高处理行为过程的透明度,以此保障用户对其个人信息的控制权和决定权。个人信息保护机制是保护个人信息最普遍的企业格式文本,本应贯彻告知同意规则。但是,在线平台企业落实告知同意规则一直是一个难题,尤其是在乱象丛生的移动平台应用程序领域。在该领域,因缺乏智能化程序机制,告知同意规则在复杂的数据利用中难以被有效执行:首先,在线平台企业通过格式化的个人信息保护政策(隐私保护政策)回避应向用户承担的部分法定义务,用户不得不接受不平等的网络信息交易契约,包括服务协议、可接受使用政策以及第三方合作名单。这令告知同意规则在事实上成为摆

设。其次, 用户通常只能在首次使用时一次性概括同意个人信息保护政策的内容, 这使得单独同意、书面同意和撤回同意沦为概括同意的附属物。再次, 部分在线平台企业制定的个人信息保护机制中的信息收集条款仅涉及个人信息处理者一般性的权利义务, 且未约定任何的责任条款, 而鉴于个人信息的人格属性, 其损害后果往往较为严重且无法弥补^[8]。此时, 通过个人信息保护机制维护个人信息权益的目的基本落空。此外, 当前平台的个人信息保护机制在面对个人信息过载及其规模效应、数据聚合效应等诸多挑战时^[9], 由于告知同意规则的程序机制难以适应数据处理算法的迭代更新, 未根据不同场景下的告知同意强度设置差异化的程序机制, 需要同时满足“充分告知”和“简单易懂”的要求。最终, 差异化保护的落空使得在线平台企业负担过重而无力实质性解决个人同意的一系列问题。

第三, 未能将保护敏感个人信息的技术要求真正落地。公众对个人信息敏感性的感知是由信息处理的场景所决定的。换言之, 个人信息的敏感性既取决于个人信息的性质或类型, 又取决于其处理场景, 即是否属于个人敏感信息需要结合相应的处理场景作出判断。例如, 手机号通常不是敏感个人信息, 人们乐于在亲友之间分享手机号, 但对于将手机号公之于众则十分抗拒, 因而公之于众的手机号可能构成敏感个人信息。对于那些通常不属于敏感个人信息但在特定处理场景中会呈现敏感性的个人信息, 可称之为“相对敏感个人信息”^[10]。目前, 在线平台企业大多没有完整列明所处理的敏感个人信息类别, 企图通过“等”来获得概括授权。鉴于有关敏感个人信息保护的法律规定大都没有体现应有的风险管理理念, 在线平台企业的个人信息保护政策鲜有保护敏感个人信息所需要的技术合规措施, 平台在程序机制方面对敏感个人信息保护的技术应用多停留在理论探讨阶段, 未在其产品中根据在线平台企业对个人信息处理的特殊情况设置直接触发用户个人信息撤回等方式, 也未在平台运行中基于不同类型的特殊处理场景采取分别勾选、单独弹窗等形式实现对敏感个人信息的风险

预防和动态保护。

(二) 平台个人信息保护机制存在欠缺的原因

平台个人信息保护政策在贯彻《个人信息保护法》基本原则、践行告知同意规则和保护敏感个人信息时面临上述种种不足, 其背后的深层次原因在于对程序机制的重视程度不够, 尤其是未能通过信息科技对个人信息保护政策程序机制进行塑造和完善, 发挥其在个人信息全生命周期保护中动态且有效的“超助推”^[11]作用。

第一, 个人信息保护政策的实施暂未启用技术措施保障程序机制的有效运行。在信息脱离权利主体支配的数字时代, 随着数字技术的发展, 数字技术完全可以越过人格化的同意, 形成对同意的技术强制。以主体为基础的同意制度无法应对数字技术风险的算法规制, 正如诺斯曾言: “如果将作为人格化交易之基础的‘一致同意’的意识形态作为单纯的互惠是错误的, 那么在一致同意的条件下, 正式的交换规则和监督都被最小化了。”^[12]真实场景下平台用户的个人同意在复杂的个人信息处理过程中往往形同虚设, 尤其是在没有技术保障措施帮助用户撤回同意的情况下。例如在安徽美景信息科技有限公司与淘宝(中国)软件有限公司不正当竞争纠纷一案中^②, 淘宝用户缺乏撤回同意的程序机制, 无法根据自己的意愿撤回淘宝公司处理其个人信息的授权。随着代码程序和算法设计的不断迭代, 根据不同场景区分同意强度已经可以实现。技术作为制度因应中的优先选择^[13]可发挥程序、指令和数据对程序机制的塑造作用, 避免用户在知觉定式下陷入概括同意的侵权风险。

第二, 个人信息保护政策对个人信息权利^[14]行使中程序节点的静态因应。数字技术正以惊人的速度在发展, 其求利性极大地增加了个人信息保护的难度。个人信息保护政策若不引入更为动态的程序, 则难以保障用户在平台个人信息处理活动中有效行使权利。例如在朱烨诉百度案中, 法院在当时的法律框架和理论依托下作出保护在线平台企业的判断, 选择拒斥朱烨的同意权, 肯定百度搜集数据痕迹的“特权”地位^[15]。这是作为权利运行起点要件的同意规则难以有效执

行的现实写照,也映衬出否认数据痕迹人格特性和用户同意“名存实亡”^[16]的数字生态。当前的数字生态表现为:个人作为应用平台的用户,既是消费者也是生产者,个人用户作为企业生产激励的一员,不得不接受平台的个人信息保护方法,包括个人信息第三方使用清单、可接受使用政策以及服务等级协议。因个人信息保护机制格式文本设置的不平等条件,以及个人信息权利相关的动态化程序缺失,个人信息权益的保护已被湮没在数字技术的丛林之中。

第三,个人信息保护的程序机制发展路径面临“道高一尺,魔高一丈”^③的困境。在数字生态中,面临法律之“道”难以企及技术发展之“魔”的困境,法律与数字技术的嵌入式发展可能是有效的破解之法。个人信息的程序机制发展路径主要表现在个人信息全生命周期管理的实践之中。国外平台企业的个人隐私信息管理实践经历了“公平信息实践”^[17]、“隐私影响评估”^[18]和“隐私保护设计”^[19]三个不同的发展阶段。这对于我国在线平台企业个人信息保护实践具有借鉴意义,也一定程度上推动着我国在线平台企业在此前经验的基础上拥抱数字技术,开启个人信息保护实践的“隐私即设计”阶段。虽然我国《个人信息保护法》确立了在线平台企业应当遵守的个人信息保护制度,但在线平台企业在个人信息管理实践中仍然面临难题,主要表现在:在线平台企业的个人信息保护机构难免具有一定的经济依附性,对于个人信息权益遭受侵害往往反应滞后;个人信息保护影响评估仅停留在专门机构的经验层面,未实现技术内嵌于程序机制,进而对代码、算法运行节点进行有效规制的目的。为破解这一困境,平台个人信息保护政策亟待揭开在线平台程序运行的技术面纱,运用智能化的程序机制将个人信息过程性保护的追责视角直接指向应用程序的算法设计者,敦促作为算法权力^[20]实际控制主体的在线平台企业在处理个人信息的过程中达到实质意义上的合法合规。

二、构建个人信息保护智能合约机制的必要性与可行性

智能合约如今多指立基于区块链技术的可

编程应用。由于控制技术环境与运营环境的大型在线平台企业扼守了App运行的关键环节,其对App个人信息保护的技术设置及相关行为具有决定性作用^[21]。我国《个人信息保护法》第58条为大型在线平台企业设定了一系列特殊义务^[22]。在此规范基础上,构建个人信息智能合约机制,可以有效表达用户的利益诉求。在不能改变平台占据技术优势的情况下,智能合约这一促使交易自律的科技手段可提升个人信息保护政策的管理效能。换言之,引入智能合约技术重塑目前的个人信息保护机制,运用其不需要外部输入就可以在特定情况下执行特定程序实现特定目的的功能,能够帮助用户根据《个人信息保护法》第四章的规定动态化地行使个人信息处理活动中的权利^[23]。

(一) 个人信息保护场景下的智能合约:可控制程序节点的特殊协议

智能合约是以数字形式定义并自动执行的协议^[24]。其在本质上使用着代码语言,具有智力成果外观,也承载着交易双方的意思表示,在合同形式自由原则下,可以被理解为特殊形式的合同。当下用户与平台企业之间的关系已从单纯的消费关系转变为合作生产关系^[25],基于此种新型关系的合作协议可采用智能合约控制程序节点,保障用户的个人信息权利。

第一,智能合约具有与生俱来的程序节点控制功能,应使其具备保障程序机制有效运行的技术潜质。例如,在全国法院系统首次运用智能合约技术的案件中,原告在条件达成时通过电子诉讼服务平台的履约程序一键进入执行系统^[26]。就法律性质而言,此类智慧司法应用中的智能合约在符合我国《计算机软件保护条例》第2条所指的“计算机程序及其有关文档”独创性标准的情况下,是智力成果的结晶,其创作单位有权进行版权登记。但智能合约在合约订立的部分有着与传统合同类似的特征,具有明确规定双方权利义务关系的效力。譬如,在美国佛罗里达州南区法院判决的首个涉及智能合约效力的案件中,智能合约所代表的内容不再只是一堆代码,其自动执行及交易履行的实际效果得到了法院的认可^[27]。由此可知,智能合约是具有数字化表现形式并控

制程序节点的特殊协议。

第二, 智能合约是一种可灵活调整应用领域的创新技术, 若应用于个人信息保护的场景, 则用户与平台之间就个人信息的处理所达成的内容将外化为代码表示的个人信息保护政策及特定条件触发后的自动执行机制。以是否需经用户同意为标准, 可将个人信息保护场景下的智能合约区分为需经用户同意和无需经用户同意两种类型。一方面, 以智能合约为程序机制的个人信息保护政策并非纯粹的企业自律规则, 在许多重要情形下必须经过用户同意并取得其授权后才能发生法律效力。另一方面, 并非个人信息保护政策的所有内容都需要经过用户的同意。用户是否同意将会对其性质与效力产生较大影响。因此, 可基于智能合约具体条款是否经过用户同意分别认定其效力。概言之, 承载个人信息保护政策的智能合约在用户未同意时为在线平台企业自律规则, 经用户同意的部分为具备法律意义且不得违反法律、法规规定的合同。无论是企业自律规则还是合同, 都有智能合约程序机制保障条款的执行。

(二) 以智能合约构建程序机制保护个人信息的必要性

在用户个人信息保护不足的情形下, 智能合约技术的引入将带来“技术反哺法律”的革新效果。此时, 智能合约自动处理的可靠性能够纾解个人信息保护的现实困境。智能合约作为改变履行不确定性的特殊合约, 在面对在线平台企业进行麦克风窃听、通信录窃取、相册非授权读写、大数据杀熟等个人信息侵权行为时, 可以更大范围和更深层次地保障个人的信息权益, 发挥在救济途径方面与个人信息侵权诉讼相比更为高效的比较优势。

第一, 以智能合约构建个人信息保护的程序机制是个人信息范围扩张后实现动态保护的必然选择。我国《个人信息保护法》第4条对个人信息范围采取的是“识别+关联”的界定标准, 这使得在线平台企业在没有收集个人姓名、电话与地址, 单就用户的IP地址、MAC地址、IMEI码、浏览记录、消费记录以及种种行为信息进行收集的情况下, 仍然要使对这类信息的收集与利

用行为达到合规要求。譬如, 在微信读书案中, 读书信息作为行为信息也属于个人信息^③, 腾讯公司应当履行作为个人信息处理者的义务性规范。实践中, 不乏在线平台企业通过收集、利用上述个人信息侵犯个人信息权益的现象。例如百度网讯公司使用Cookie技术时收集用户网上活动轨迹, 在未经用户同意的情况下于合作网站上展示与之有一定关联的推广内容^④。为了全方位保护个人信息, 在通过技术来识别、评估、预防和控制个人信息侵权损害的趋势下, 引入智能合约可以在个人信息处理过程中持续拓展个人信息保护的范围, 将新增的行为信息等纳入其中给予动态化保护。

第二, 运用智能合约技术构建程序机制能为个人信息权利行使过程中程序节点的连贯融通提供解决方案。个人信息权利指包括个人信息主体知情、决定、查询、更正、复制、删除等具体权能在内的一组权利^[28]。我国《个人信息保护法》第四章对此作了具体规定, 丰富了个人信息删除权的请求情形并补充了例外规定, 同时要求个人信息处理者建立个人行使上述权利的申请受理和处理机制, 改变以往个人信息权利行使的难题。在朱烨诉百度Cookie侵犯隐私权案中, 二审法院认为百度公司作为在线平台企业提供给用户的《使用前必读》的确存在字体过小的情况^⑤。此类涉及个人信息保护的文本中的重要事项不仅字体较小, 且夹在无关文字中间, 难以保障用户的知情权。运用智能合约等技术手段可以让用户在决定个人信息权益的重要事项时获得明显的标识提醒, 来应对企业个人信息处理活动中的违规乱象, 确保个人信息相关权利的实现。同时, 智能合约能够随时基于对触发条件的自主研判而启动运行程序, 提升个人信息各项权能之间的连贯性, 不需要等待个人信息具象化侵权风险外溢而提前预防处置。此外, 智能合约承载的个人信息保护政策可以落实《个人信息保护法》第45条第3款规定的可携带权, 当条件成就时可以根据个人信息处理者提供的转移途径自动进行处理。

第三, 引入智能合约构建个人信息保护程序机制能完善个人信息权益的救济途径。由于在线

平台企业的运营自律性较差以及用户个人意愿难以有效表达,对在线平台企业违法违规处理行为的追责通常只能采取事后惩罚的方式且时间成本高昂。而对敏感个人信息的泄露或滥用可能导致当事人的人格利益严重受损,并且在互联网时代的传播条件下,相关个人信息很容易迅速遭到二次扩散,造成不可逆转的长期损害。在个人信息保护领域,通过司法裁判提供救济的方式效率较低,难以及时有效地制止系统性侵权。譬如,著名的黄某诉腾讯科技(深圳)有限公司等隐私权、个人信息权益网络侵权责任纠纷,从2019年5月17日立案到2020年7月30日作出停止微信读书收集、使用原告黄某微信好友列表信息的判决,历时超过1年,才使黄某撤回同意和删除个人信息的权利得到实现^⑨。2022年7月10日,自许昌市公安局发布的警情通报中明确宸钰信息技术有限公司删改数据、屏蔽瞒报至今,村镇银行客户的个人金融信息权益保护还有很长的路要走。与之相反,智能合约的自动执行特性在个人信息保护应用场景下可以在短时间内针对违规处理行为以自动提示撤回同意和点击删除个人信息的方式对同类问题进行及时救济,避免法院诉累并节约司法资源,是对个人信息权益侵害进行救济的新途径。

(三) 构建智能合约个人信息保护程序机制的可行性

随着操作系统、应用程序及其分发平台的广泛应用,在线平台企业强制授权、过度索权、超范围收集个人信息的问题备受重视。为改变对个人信息处理者追责机理模糊化、治理节点滞后的现状,运用智能合约程序机制解决上述问题时,需对智能合约进行技术与内容两方面的针对性设计。在技术方面,智能合约对个人信息保护政策的程序机制进行完善,必然需要对区块链与个人信息保护规范之间的冲突进行调和。在内容方面,应在充分界定目标用户和服务内容的基础上,运用智能合约设置不同层次和强度的同意选项。如此才可发挥智能合约的功能,即实现个人信息“全生命周期”的动态保护,并通过在线平台企业违反个人信息保护政策后自动进行追责的执行功能,让用户获得更为有效的救济。

第一,根据个人信息保护规范的要求对区块链应用进行定制化开发,可使此类区块链应用的智能合约具备构建个人信息保护政策程序机制的技术基础。众所周知,区块链智能合约是目前最常见的智能合约,但由于区块链智能合约的每个节点都对应着一个用户,只要用户拥有公钥(公共分类账上显示的匿名用户地址)、私钥(用于授权交易的密码)和令牌就可以获知节点上分布的所有信息^[29]。这意味着区块链技术与个人信息保护规范之间存在冲突。在面对此冲突时,个人信息保护场景下的智能合约必须对区块链技术进行相应的改进,定制化地开发承载智能合约并保护个人信息的区块链应用。同时,用户与在线平台企业形成的合意由 CLACK 标准语言生成对应的合约代码并即时嵌入 Cookies,以此按照用户意志即时过滤被收集的个人信息^[30]。此举既可以控制在线平台企业实施个人信息处理行为的自由度,又可以让用户意志获得强有力的保障。此时,智能合约程序机制堪比智能的数据保护官,在企业合规层面改变用户使用企业服务时容易招致不公的“点击即成立”模式,高效地实现企业的自我监督^[31]。

第二,通过智能合约的条件触达自动弹窗等功能完善个人信息保护政策的程序机制。在我国《个人信息保护法》公布之前,在线平台企业大多学习欧美经验使用“隐私政策”(privacy policy)一词。随着《个人信息保护法》的颁行,在线平台企业围绕双清单目录等对隐私政策进行修改,或更名为个人信息保护政策。但在实践中,冗长的个人信息保护政策缺乏与之配套的实施机制,同时,用户也有着通过技术控制个人信息的智能辅助需求。为更好地保护用户的个人信息权益并实现个人信息保护政策由格式化向个性化转变,需要运用技术搭建企业与用户平等对话的桥梁,以改变现实生活中在线平台企业滥用权限侵害个人信息的乱象。从切实落实个人信息保护有效性的角度而言,“技术+个人信息保护”的模式可通过技术加压打造个人信息保护的坚固防护网,构设出一个更加科学合理的保护机制。其中,重点在于引入技术实施机制,包括运用智能合约承载并实施个人信息保护政策。个人信息

保护政策在严格执行双方当事人意思并有效实现同意的过程中, 既能够发挥促进个人信息处理者自律的功效, 又可以满足用户对于个人信息保护的归责需求。在线平台企业通过隐私保护政策等举措实施的低效自我规制将被运用智能合约的个人信息保护政策所替代。

三、智能合约程序机制与《个人信息保护法》的对接

个人信息处理活动本质上是一种技术应用活动, 不同于一般的行为治理, 必须进行技术治理^[32]。智能合约程序机制对接《个人信息保护法》, 可从贯彻个人信息保护基本原则、实现有效同意、对接个人信息处理者义务性规范和提升敏感个人信息相关条文的适用效果等四个层面展开阐述。

(一) 贯彻个人信息保护的基本原则

我国《个人信息保护法》的基本原则是在线平台企业处理个人信息时应当遵循的基本准则, 包括“合法、正当、必要和诚信原则”“责任原则”和“公开透明原则”等^⑤。作为对个人信息保护政策进行迭代升级的技术应用, 智能合约程序机制以“信息科技规制信息行为”为设计理念, 是贯彻《个人信息保护法》基本原则的关键举措。在智能合约程序机制与个人信息保护基本原则的衔接上, 《个人信息保护法》第9条规定的“责任原则”要求个人信息处理者应当采取必要措施保护个人信息安全。这为运用智能合约程序机制落实个人信息保护基本原则预留了解释空间。在个人信息保护政策的执行过程中, 必须借助对原则的具体化, 方能在具体规则与基础价值之间形成“有意义的彼此联系”^[33]。譬如, 智能合约程序机制可对违反《个人信息保护法》第6条第2款“必要原则”的行为进行前置性预防: 在非服务所必需或无合理场景的情形下, 避免以所谓积分、奖励、优惠等方式欺骗诱导用户提供身份证号码等个人信息^⑥。此外, 根据《个人信息保护法》第7条公开透明原则的要求, 智能合约程序机制可通过预定条件下的动态弹窗方式

对个人信息处理活动的重要事项予以全面披露, 保证用户对重要事项的知情与理解^[34]。总体来看, 以智能合约为程序机制的个人信息保护政策能够从业务流程设计开始就嵌入个人信息保护的基本原则, 通过系统的技术设定、代码架构的调试等, 让抽象的《个人信息保护法》基本原则形成更为具体的个人信息权益保护效果。

(二) 对接信息处理行为的义务规范

基于个人信息处理时呈现的个人权益的微妙性和复杂性, 我国《个人信息保护法》创设了一种独特的系统保护机制, 为个人信息处理者的处理行为设定了多个层面的义务规范。智能合约程序机制可与个人信息处理者的一系列义务规范相衔接, 主要包含以下四个方面: 第一, 在个人信息处理活动的安全措施方面, 《个人信息保护法》第51条具体列举了保护个人信息应当采取的安全技术措施, 并对个人信息的技术治理作了框架性规定, 为企业在个人信息保护政策实施中运用智能合约提供了规范依据。第二, 在个人信息保护责任主体方面, 《个人信息保护法》第52条规定大型在线平台企业应设立个人信息保护负责人, 第53条还规定须有专门机构或指定代表。但在没有技术辅助的情况下, 上述主体都难以对个人信息处理活动进行有效监督, 而智能合约则是与此类组织的监管需求相匹配的技术。第三, 在个人信息保护影响评估方面, 《个人信息保护法》第55、56条以常态化的影响评估确立了在线平台企业的自我规制和风险管理模式。智能合约正好能顺应个人信息保护影响评估制度的动态特性, 帮助在线平台企业动态监测个人信息的潜在风险, 并采取对个体影响最低的方式处理个人信息。第四, 在个人信息处理者的特别义务方面, 《个人信息保护法》第58条对提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者(如腾讯、阿里等)规定了特别义务, 而信息量较少、处理活动简单、技术水平较低的小型在线平台企业则应当遵守个人信息处理者的一般义务。智能合约可从技术层面落实不同类型处理者的保护责任, 监督在线平台企业对个人信息实行分类管理、去标识化等安全技

术措施,确保应用程序操作权限的可控授权与应急预案的有效执行。

(三) 承载并丰富告知同意规则的程序内容

智能合约程序机制可充实并丰富告知同意规则所亟需的程序内容,拓展个人同意相关的代码程序运行空间。我国现行《个人信息保护法》确立了个人信息处理上多元而非一元的同意规则^[35]。其中,作为同意规则重要条款的第16条规定,个人信息处理者“不得胁迫同意”。但在用户遭受在线平台企业“胁迫同意”的情形时,往往缺乏申诉反馈的途径。这主要在于多元同意规则具有形态差异化特性,当其面对作为科技活动的个人信息处理行为时,缺少差异化的程序机制予以区别对待。进一步而言,尽管《个人信息保护法》明确规定在线平台企业等处理者在处理个人信息时的告知同意义务,但难以应对个人信息应用场景的日益多样化。为了避免个人信息处理者在不起眼之处标识“一经使用即同意授权”,解决用户不开启与业务功能无直接关系的部分敏感信息收集权限就无法使用的“二选一”困境,智能合约程序机制可从程序运行方面加强对个人信息处理行为的监督,推动在线平台企业个人信息保护政策得到贯彻落实。《个人信息保护法》第14条第1款对告知同意规则的有效要件作出“须具备同意能力、同意系在充分知情的前提下作出、真实自愿及明确具体等”的规定,其具体构成包括:第一,同意能力,即一个人对其决定的性质、程度以及可能产生的后果的理解能力。第二,充分知情。由于在个人信息处理活动中,处理者与个人之间的信息是不对称的,因此同意规则必须与告知规则密切联系,即要求处理者必须充分告知,从而确保个人在充分知情的前提下作出同意的决定。第三,自愿具体。即个人信息处理者通过欺诈、胁迫或者误导等方式取得的个人同意是无效的。基于贯彻实质重于形式的同意逻辑,智能合约程序机制内嵌的个性化拟制、自动弹窗等技术可承载并完善告知同意规则的程序内容,保障用户对个人信息控制与决定。并且由于智能合约程序机制最多禁止或限制合同的履行,而非否认个人信息协议内容本身效力,因此对在线平台企业处理者的自主经营权予以

了最大程度的尊重。

(四) 提升敏感个人信息相关规范的适用效果

设立个人信息保护政策的智能合约程序机制能矫正个人相对于信息处理者的弱势地位,事关敏感个人信息保护的有效性。我国《个人信息保护法》第28条规定了个人信息处理者对敏感个人信息采取严格保护措施的义务,但29条所规定的敏感个人信息单独同意制度暂无可靠的实施机制。针对敏感个人信息相关同意规则的要求,智能合约在提供单独同意的弹窗机制时,能让用户以电子化形式实现敏感个人信息的书面同意。因此,探索“智能合约技术+个人信息保护”的方案是实践中提升敏感个人信息保护规范适用效果的重要途径。在收集、存储与应用人脸、指纹、视虹膜、基因等敏感个人信息的过程中,一旦发生个人信息侵权,在短时间内就可造成极大影响,且事后难以进行有效救济。而《个人信息保护法》第28条第1款列举的各项信息因具有涵括性而不能直接作为认定依据,是否属于敏感个人信息仍需根据具体场景判定^[36]。为顺应敏感个人信息的动态化保护需求^[37],智能合约程序机制可根据敏感个人信息和一般个人信息的判断条件识别出个人信息的不同类型,为用户提供相应的差异化保护。这既可降低对一切个人信息无差别保护所带来的高昂成本,又能提升特殊类型个人信息的保护标准,有效平衡个人信息的保护与利用。此外,智能合约程序机制可实时监督平台对生物识别、行踪轨迹等敏感个人信息采取严格保护措施的实施情况,并根据合约条款向用户反馈结果。

四、企业个人信息保护政策中智能合约程序机制的实现条件

智能合约程序机制在在线平台企业个人信息保护政策中的实现,有赖于强有力的组织保障、可靠的技术基础和具有操作性的实现机制。首先,需要依据我国《个人信息保护法》第52条规定的“个人信息保护负责人”制度并借鉴欧盟《一

般数据保护条例》中“数据保护官”(DPO)^[38]制度的有益经验,设立以技术人员为主体的在线平台企业个人信息保护负责人制度。同时,根据《个人信息保护法》第58条第1款中设立“独立机构”监督企业个人信息保护情况的规定,将上述个人信息保护负责人作为该独立机构的成员,为智能合约程序机制的构建提供组织保障。其次,基于区块链在个人信息保护领域的重大应用前景^⑦,个人信息保护负责人对作为智能合约底层技术的区块链进行针对性改造,设计符合个人信息保护规范要求的区块链,奠定构建智能合约程序机制的技术基础。最后,个人信息保护负责人通过智能合约构造“事前—事中—事后”程序机制,为个人信息保护政策的实行提供切实可行的实施方案。

(一) 强有力的组织与人员保障

经由对控制理论、经济上的合理性以及现实中的必要性等多方考量,我国《个人信息保护法》部分借鉴了欧盟《数字市场法(草案)》《数字服务法(草案)》关于大型在线平台和数字中介服务提供者的规定^[39],设置了在线平台企业个人信息保护的特别义务,为个人信息处理行为的技术治理奠定了规范基础。其中,《个人信息保护法》第58条在个人信息保护治理节点中引入新的主体,进而运用智能合约等新的工具提供规范依据。该条给达到一定条件的在线平台企业设定了自我规制义务,具体包含成立监督个人信息保护情况的“独立机构”、制定保护个人信息的“平台规则”等。在上述义务的履行中,对个人信息处理行为进行技术层面的专门监督尤为重要。这也与《个人信息保护法》第52条的规定相契合。该条规定,达到国家网信部门规定条件的在线平台企业负有任命个人信息保护负责人的法定义务。此负责人可以是在线平台企业的工作人员,若在线平台企业本身没有合适的人选,也可以通过与其他专业服务组织订立协议,由该组织为其提供合适的人来担任个人信息保护负责人^[40]。根据在线平台企业落实个人信息保护政策的现实情况,还可选择任命个人信息保护的内部负责人和外部负责人共同履职。而无论是内部还是外部负责人,将擅长技术的人作为个人信息保护负责人,

发挥其运用信息技术保护个人信息的优势已经成为一种趋势。这点可以借鉴德国企业任命信息技术部等非管理人员担任数据保护官的相关经验^[41]。同时,个人信息保护负责人应当是《个人信息保护法》第58条中监督个人信息保护情况的独立机构的组成人员,即将满足一定资质条件进行智能合约编程开发的技术人员作为独立机构的成员,负责用技术手段监督个人信息保护政策的执行情况。其任命的条件既要包括正高级职称等专业认定的资质要求,也要满足熟练运用区块链智能合约等技术保护个人信息的实践能力要求。

此外,上述个人信息保护负责人应当负有专项工作任务,发挥其包括掌握智能合约应用在内的技术专长,为平台用户行使个人信息权利建立受理和处理的程序机制。基于此,个人信息保护情况的监督机构通过控制系统的代码就可实现规制,进而实现控制目的^[42]。为了达成这一目标,个人信息保护负责人的人员构成和职责范围有必要进行如下完善:其一,为了保障监督机构的独立性,确保个人信息保护负责人能够完成智能合约程序机制的构建,进而实现个人信息保护政策全流程落地监控的目标,应参考我国《互联网平台分类分级指南(征求意见稿)》和《互联网平台落实主体责任指南(征求意见稿)》^[43]等官方文件对在线平台企业类型、主体责任的划分,将在线平台企业细分为操作系统平台、应用商店、小程序平台和电商平台等^[44],根据不同类型对个人信息保护负责人构成来源中的内部和外部人员所占比例进行灵活调配,以此兼顾个人信息保护负责人的独立可靠与在线平台企业的经济可负担性。其二,在职责范围方面,由于此类掌握智能合约编程技术的专家在平台企业个人信息处理行为的技术监督方面具有相对优势,在执行个人信息保护政策的各个环节中可以履行以下监督职责:①负责制定个人信息保护政策中运用智能合约完善程序机制的具体方案;②负责通过智能合约程序机制监督个人信息加密、去标识化等安全技术措施的实施情况;③负责运用智能合约程序机制对个人信息处理行为违背操作权限和操作规程的情况进行监控;④为智能合约提供

运维服务,保证其动态提醒用户关注个人信息保护的监测结论;⑤为智能合约在条件触发下启动执行措施提供技术保障。

(二) 可靠的技术基础

智能合约作为技术治理的手段之一,在实现个人信息保护政策过程中至关重要。传统模式的智能合约不借助区块链技术,仅仅是在特定情况下执行特定程序实现特定目的的计算机编程,在理论上能够提高个人信息处理的安全性并降低时间成本。区块链模式下的智能合约则是存储在区块链上的一段代码,是区块链下层信息逻辑链式关系与上层服务沟通的渠道,经由区块链数据库写入和读取,并由相应事件予以触发^[45]。区块链技术作为一种具有普适性的底层技术架构^[46],可以强化对信息主体的保护,实现通过信息科技手段科学管理和规范个人信息交易的目标^[47]。但由于个人信息保护规范的抽象性与核心概念的不确定性^[48],去中心化架构的区块链与个人信息保护规范存在一定程度的冲突与抵牾,为构建个人信息保护政策的智能合约程序机制,需要对区块链技术加以改造,使其符合个人信息保护规范的要求。

为使区块链智能合约与个人信息保护规范的要求相适应,需要对区块链技术进行四个方面的调适:首先,采用私有链或联盟链的架构,使得个人信息保护负责人以中心化的方式对区块链进行直接管理。其次,鉴于本文第二部分提及的个人信息存储在区块链上存在的透明化风险,改造区块链的重点在于建立个人信息的“非明文存储原则”。为贯彻该原则,实现信息上链后其他主体无法知晓其中内容的技术目标,可在非对称加密等通用加密方式的基础之上采用冻结数据的加密机制强化保密,即在区块链上进行登记,通过附加信息来确定哪些信息已被冻结,以及查找、识别特定信息。再次,由于区块链难以保证目的限制与最小化的规范要求,可对区块链采用“零知识证明”技术以解决此问题。“零知识证明”可以看作是一种协议,通过该协议能够在不使用任何密码或其他敏感数据的情况下实现数字身份验证,推动区块链数据最小化的实现,使

得移动端也可以即时同步区块链数据^[49]。最后,为保障在区块链上实现用户个人信息的删除权,将个人信息存储在单独的“脱链数据库”中或采用删除解密密钥的方案,可使区块链符合此项权利的行使^[50]。

(三) 可操控的实现机制

智能合约程序机制对个人信息保护政策的实现遵循“事前防范一事中规制一事事后处置”的建构理念。对此,智能合约程序机制可以发挥其所具备的个性化拟制和动态化控制功能,推动个人信息保护政策的有效落地。在合约条款中明确敏感个人信息的认定标准,设计单独同意、书面同意和重新同意的自动弹窗提示机制,并为用户自由设定个人信息处理方式提供多元途径,对个人信息处理中的违法违规行为自动进行救济。一方面,用户可通过事前事中的程序机制实现过程性控制,进而形成对侵权行为的预防。另一方面,用户可通过事后的程序机制自动采取措施及时制止侵权行为,以防止个人信息权益损害后果的扩大。

1. 事前机制:基于智能合约的用户个性化设定程序

个人信息保护政策的事前阶段是在线平台企业获得用户授权与收集用户个人信息的阶段。在这一阶段,可构建基于智能合约的用户个性化设定程序作为事前程序机制。其理由在于,虽然不少在线平台企业已对个性化推荐与个性化广告管理给出了关闭或开启的具体指引,但在事前阶段,在线平台企业在敏感个人信息的收集与敏感权限的设置方面存在概括授权的问题,即当用户授权了位置信息的使用之后,APP所有与位置相关的服务都获得授权^[51]。在线平台企业个人信息保护政策的实质合规与否直接关系到是否有效保护了用户的个人信息。技术加持的个人信息保护政策可通过智能合约完成事前阶段的个性化设置,不断拓展用户在合约内容方面的自定义范围,实现个人信息保护政策的事前实质化协商。在协商过程中,用户可通过智能合约实现在不同领域对其个人信息的收集、利用进行个性化的授权,包括选择被收集、利用的个人信息类型和范

围,并形成相应的记录供用户查询、复制和删除。概言之,关注用户个人信息的保护需求是注意力经济时代的重点,作为事前机制的个性化设定程序可为用户提供多元选择模式,充分保护用户的个人信息权益。

2. 事中机制: 重大事项自动提示与选择程序

个人信息保护政策的事中阶段是在线平台企业对信息进行存储、使用、加工、传输等处理的时段。为在此阶段实现个人信息保护政策,需要个人信息保护负责人将技术与法律深度融合,通过智能合约的代码编程,设计出兼顾用户体验和个人信息保护实效的程序机制,规制在线平台企业在应用程序运行中的个人信息处理行为。具体而言,利用智能合约程序机制将互联网应用程序和操作系统中原有的隐私政策进行数智化升级,推动产品指引、Cookie 政策、SDK 和第三方目录等核心内容适应智能合约技术带来的适用革新。在这一阶段应当构建重大事项自动提示与选择程序,主要包括: 第一,为 Cookie 与 SDK 技术提供动态化的弹窗说明,介绍该平台使用了哪些 Cookie 技术,并以通俗易懂的语言向用户说明使用 Cookie 技术的目的,告知用户管理 Cookie 的步骤以及关闭 Cookie 后的影响。同时,根据我国《个人信息安全规范》的规定,围绕 SDK 这类由运营商委托第三方开发的软件开发工具包,提前在智能合约中订立病毒传播、违法收集个人信息、泄露隐私等安全风险的应急处理条款。第二,当在线平台企业需要收集用户敏感个人信息时,启动事中程序提示用户并识别即将收集的个人信息及其合法性。譬如,我国《个人信息保护法》第 29 条以及《个人信息安全规范》都对个人敏感信息和生物识别信息提出了单独告知并征得明示同意的要求,智能合约程序机制可在个人敏感信息和生物识别信息处理时自动弹窗单独告知并提供明示同意按键以供选择。第三,在对外委托和提供信息时自动弹窗说明获知渠道,在发生任何可疑的变化时发出预警^[52],保障用户在个人信息处理过程中及时了解在线平台企业将采取哪些措施保证信息的安全性以及信息流转、处理活动的合法性。根据我国《个

人信息保护法》第 23 条规定提出的“详细披露+单独告知”要求,提供专门渠道了解在线平台企业提供信息前第三方的数据管理情况,提供信息时的传输方式,提供信息后的监督和审计等。考虑到按传统方式进行披露可能会导致篇幅较长,采用智能合约程序机制可实现对在线平台企业冗长、晦涩难懂的隐私政策进行重大技术升级,即通过自动弹窗提示知情途径,引导用户自由选择专项披露文件以获知详情。

3. 事后机制: 处理行为违法违规的自动执行程序

个人信息保护政策的事后阶段是指在线平台企业处理个人信息时出现违法违规行为后的时段。由于自动化技术对个人信息的自动处理愈发普遍^[53],用户对个人信息的保护有着更加紧迫的时效性需求。在事后阶段,个人信息保护负责人运用智能合约设计事后程序机制,以自动化方式应对个人信息侵权行为可解此燃眉之急。而这有赖于个人信息保护负责人通过智能合约程序机制设计针对个人信息处理行为违法违规的自动执行程序。譬如,在智能合约订立时就制定“默认+自定义”相结合的自动执行方案,通过为用户删除信息、更改隐私设置或者在系统中关闭设备权限功能等提供高效便利的机制,当违法违规行为触犯条件后自动对个人信息进行删除或者匿名化处理,以技术向善推动在线平台企业自律。当发生个人信息侵权行为时,自动执行程序根据具体侵权行为的不同严重程度,按照提前拟定的条款或设置的个性化选项,自动在设备的设置功能中开启或关闭地理位置、通信录、摄像头、麦克风、相册、日历等权限,提供用户改变授权范围或撤回授权的选项。此外,运用智能合约对特别严重的个人信息权益侵害行为,根据用户提前设置的条款,自动删除该用户在平台数据库中的个人信息,随即撤回对该平台的全部授权。为保障用户在平台违法违规后可进行个人信息的迁移,自动执行程序根据用户提前选择的实施方案导出个人信息至本地端,同时,清理该用户在平台数据库中未匿名化处理的个人信息,甚至在条件触发时显示在线纠纷化解平台的操作指

引以助力用户维权。

五、结语

尽管我国《个人信息保护法》为在线平台企业等个人信息处理者设置了规范系统的保护义务,但上述主体在个人信息处理中仍存在违法违规行爲,给个人信息权益带来巨大的侵害风险。值《移动互联网应用程序信息服务管理规定》颁行之际,为智能合约等技术治理手段在《信息安全技术移动智能终端的移动互联网应用程序(App)个人信息处理活动管理指南》和《信息安全技术应用商店的移动互联网应用程序(App)个人信息处理规范性审核与管理指南》两部国家标准的制订中提供妥适安排恰逢其时。未来可对智能合约保护个人信息的技术标准作逐步积累,在预留技术填补的立法空间中渐进吸纳运用智能合约程序机制保护个人信息的实践经验,推动个人信息保护的具体监管机制细化,促进个人信息权益的有效保护。本文致力于探索在线平台企业参与个人信息保护技术治理的新思路,对在线平台企业的自主管理失灵进行体系改进和科技赋能,以实现一种更加有效而全面的个人信息权益保护,为用户个人信息的差异化保护需求提供一种符合代码和算法运行规律的保护方案。

注释:

- ① 我国《个人信息保护法》第5条规定:“处理个人信息应当遵循合法、正当、必要和诚信原则,不得通过误导、欺诈、胁迫等方式处理个人信息。”该条明确了个人信息处理中应当遵循的合法、正当、必要和诚信原则。《个人信息保护法》第6条首次对目的限制原则作出详细的规定,即个人信息处理者应当使用清晰的、明确的言辞表达处理目的。该条第2款还专门对收集个人信息这一处理活动中应当限于实现处理目的的最小范围作出规定。《个人信息保护法》第7条规定的公开透明原则要求个人信息处理者应通过清晰易懂的语言向个人告知相应的事项。《个人信息保护法》第9条规定责任原则,对个人信息处理活动采取问责制,处理者是个人信息处理活动的首要的责任主体,应当对其个人信息处理活动负责。该条还规定安全原则,即个人信息处理者应当采取必要措施保障所

处理的个人信息的安全,防止出现个人信息的泄露或者被窃取、篡改、删除。

- ② 参见浙江省杭州市中级人民法院(2018)浙01民终7312号民事判决书。
- ③ 参见北京市互联网法院(2019)京0491民初16142号民事判决书。
- ④ 参见南京市中级人民法院(2014)宁民终字第5028号民事判决书。
- ⑤ 我国《个人信息保护法》在第一章“总则”中以6个条文(第5-10条)对个人信息保护法的基本原则作出了规定,包括:合法、正当、必要、诚信、目的限制、公开透明等原则。详见程啸:《论我国个人信息保护法的基本原则》,载《国家检察官学院学报》2021年第5期。
- ⑥ 参见《工业和信息化部关于开展纵深推进APP侵害用户权益专项整治行动的通知》(工信部信管函(2020)164号)。
- ⑦ 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明确提出“把区块链作为核心技术自主创新重要突破口”“探索利用区块链数据共享模式”。

参考文献:

- [1] 工业和信息化部.《工业和信息化部关于开展信息通信服务感知提升行动的通知》(工信部信管函(2021)292号)[EB/OL].(2021-11-01)[2022-02-25].http://www.gov.cn/zhengce/zhengceku/2021-11/06/content_5649420.htm.
- [2] 国家互联网信息办公室、工业和信息化部、公安部、市场监管总局. App违法违规收集使用个人信息行为认定方法(国信办秘字(2019)191号)[EB/OL].(2019-12-20)[2022-02-25].<http://www.scio.gov.cn/xwfbh/xwfbh/wqfbh/42311/44109/xgzc44115/Document/1691066/1691066.htm>.
- [3] 北京微梦创科网络技术有限公司. 微博个人信息保护政策[EB/OL].(2021-11-01)[2022-02-25].<https://weibo.com/signup/v5/privacy?inviteId=598581947>.
- [4] 北京微播视界科技有限公司.“抖音”隐私政策[EB/OL].(2021-11-01)[2022-02-25].<https://www.douyin.com/agreements/?id=6773901168964798477>.
- [5] 张新宝. 个人信息处理的基本原则[J]. 中国法律评论, 2021(5): 18-27.
- [6] 许可. 个人信息治理的科技之维[J]. 东方法学, 2021(5): 57-68.
- [7] 最高人民法院司法案例研究院. 遭遇大数据杀熟? 别怕! 人民法院为你保驾护航[EB/OL].(2021-07-05)

- [2022-02-25]. <https://mp.weixin.qq.com/s/LHrADPJhbRJ5znSvjKiKzw>.
- [8] 万方. 个人信息处理中的“同意”与“同意撤回”[J]. 中国法学, 2021(1): 167-188.
- [9] 吕炳斌. 个人信息保护的“同意”困境及其出路[J]. 法商研究, 2021, 38(2): 87-101.
- [10] 孙清白. 敏感个人信息保护的特殊制度逻辑及其规制策略[J]. 行政法学研究, 2022(1): 119-130.
- [11] YEUNG K. “Hypermudge”: Big Data as a mode of regulation by design[J]. Information Communication & Society, 2017 (1): 118-136.
- [12] 道格拉斯·C. 诺斯. 制度、制度变迁与经济绩效[M]. 刘守英, 译. 上海: 上海三联出版社, 1994: 182.
- [13] 许可. 数据交易流通的三元治理: 技术、标准与法律[J]. 吉首大学学报(社会科学版), 2022, 43(1): 96-105.
- [14] 申卫星. 论个人信息权的构建及其体系化[J]. 比较法研究, 2021(5): 1-13.
- [15] 温昱. 搜索引擎数据痕迹处理中权利义务关系之反思——以两起百度涉诉案例为切入点[J]. 东方法学, 2020(6): 34-46.
- [16] 夏庆峰. 网络空间个人信息保护的通知义务完善与动态匿名化[J]. 江汉论坛, 2022(3): 95-103.
- [17] 丁晓东. 论个人信息法律保护的思想渊源与基本原理——基于“公平信息实践”的分析[J]. 现代法学, 2019 (3): 96-110.
- [18] 弓永钦. 国际企业数据隐私管理标准研究[J]. 技术经济与管理研究, 2016(8): 76-80.
- [19] 占南. 重大疫情防控中的个人信息保护研究——基于隐私保护设计理论[J]. 现代情报, 2021(1): 101-110.
- [20] 韩万渠, 韩一, 柴琳琳. 算法权力及其适应性协同规制: 基于信息支配权的分析[J]. 中国行政管理, 2022(1): 33-39.
- [21] 程啸. 个人信息保护法理解与适用[M]. 北京: 中国法制出版社, 2021: 446-447.
- [22] 王利明. 《个人信息保护法》的亮点与创新[J]. 重庆邮电大学学报(社会科学版), 2021(6): 1-13.
- [23] 程啸. 论我国个人信息保护法的基本原则[J]. 国家检察官学院学报, 2021(5): 3-20.
- [24] 郭上铜, 王瑞锦, 张凤荔. 区块链技术原理与应用综述[J]. 计算机科学, 2021(2): 271-281.
- [25] 包晓丽. 二阶序列式数据确权规则[J]. 清华法学, 2022(3): 60-75.
- [26] 北京市高级人民法院. 全国首例! 北京互联网法院采用区块链智能合约技术实现执行“一键立案”[EB/OL]. (2019-10-08) [2022-02-25]. <https://mp.weixin.qq.com/s/Eo0xxRyormAjbwg2MMgLZA>.
- [27] 李西臣. 区块链智能合约的法律效力——基于中美比较法视野[J]. 重庆社会科学, 2020(7): 73-88, 2.
- [28] 王锡锌. 国家保护视野中的个人信息权利束[J]. 中国社会科学, 2021(11): 115-134, 206-207.
- [29] NATHAN FULMER, FULMERN. Exploring the Legal Issues of Blockchain Applications[J]. Akron Law Review, 2019(1): 52-58.
- [30] 郭如愿. 论个人信息的智能合约保护——立基于智能合约的民事合同属性[J]. 西北民族大学学报(哲学社会科学版), 2020(5): 59-70.
- [31] LOTHAR DETERMANN. Determann’s Field Guide to Data Privacy Law: International Corporate Compliance [M]. Massachusetts: Edward Elgar Press, 2017: 5.
- [32] 刘永谋. 技术治理的哲学反思[J]. 江海学刊, 2018(4): 46-52.
- [33] 卡尔·拉伦茨. 法学方法论[M]. 陈爱娥, 译. 北京: 商务印书馆, 2015: 349.
- [34] 衣俊霖. 论个人信息保护中知情同意的边界——以规则与原则的区分为切入点[J]. 东方法学, 2022(3): 55-71.
- [35] 萧鑫. 个人信息处理的多元同意规则——基于同意阶层体系的理解和阐释[J]. 政治与法律, 2022(4): 158-176.
- [36] 宁园. 敏感个人信息的法律基准与范畴界定——以《个人信息保护法》第28条第1款为中心[J]. 比较法研究, 2021(5): 33-49.
- [37] 许中缘, 何舒岑. 公共卫生领域大数据治理中个人信息的利用与保护[J]. 中南大学学报(社会科学版), 2022(3): 20-31.
- [38] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Data Protection Officers(“DPOs”)[EB/OL]. (2017-10-30) [2022-04-19]. <https://ec.europa.eu/newsroom/article29/items/612048>.
- [39] EUROPEAN COMMISSION. The Digital Services Act package[EB/OL]. (2018-09-03) [2022-02-05]. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>.
- [40] 程啸. 个人信息保护法理解与适用[M]. 北京: 中国法制出版社, 2021: 410.
- [41] LOTHAR DETERMANN. Determann’s Field Guide to Data Privacy Law: International Corporate Compliance [M]. Massachusetts: Edward Elgar Press, 2017: 6.
- [42] 劳伦斯·莱格斯. 代码 2.0. 网络空间中的法律[M]. 李旭, 等译. 北京: 清华大学出版社, 2018: 6.
- [43] 国家市场监督管理总局. 关于《互联网平台分类分级指南(征求意见稿)》《互联网平台落实主体责任指南(征求意见稿)》公开征求意见的公告[EB/OL]. (2021-12-28)[2022-06-25]. <https://www.samr.gov.cn/hd/zjdc/2>

- 02110/t20211027_336137.html.
- [44] 张新宝. 大型互联网平台企业个人信息保护独立监督机构研究[J]. 东方法学, 2022(4): 37-49.
- [45] 郭上铜, 王瑞锦, 张凤荔. 区块链技术原理与应用综述[J]. 计算机科学, 2021(2): 271-281.
- [46] 王群, 李馥娟, 王振力, 等. 区块链原理及关键技术[J]. 计算机科学与探索, 2020(10): 1621-1643.
- [47] 涵铭. 个人数据使用, 期待更规范[N]. 人民日报, 2019-4-8 (18).
- [48] 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 (3): 81-95.
- [49] SHIRAZ JAGATI. Zero-Knowledge Proofs, Explained [EB/OL]. (2019-11-18) [2022-06-15]. <https://cointelegraph.com/explained/zero-knowledge-proofs-explained>.
- [50] CARLO R W De Meijer. Blockchain versus GDPR and who should adjust most[EB/OL]. (2018-10-09) [2022-06-15]. <https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most>.
- [51] 石玉珍. 网络平台隐私政策在《个人信息保护法》实施之际修订情况分析[EB/OL]. (2021-11-03) [2022-06-25]. <https://mp.weixin.qq.com/s/jdgbuYvwpiER1ei1SyzLiw>.
- [52] 雪莉·大卫杜夫. 数据大泄漏: 隐私保护危机与数据安全机遇[M]. 马多贺, 等译. 北京: 机械工业出版社, 2021: 107-108.
- [53] 田野, 张耀文. 个人信息侵权因果关系的证明困境及其破解——以相当因果关系理论为进路[J]. 中南大学学报(社会科学版), 2022(1): 58-69.

Construction of smart contract mechanism for users' personal information protection of online platform companies

XU Juan, LI Haotian

(School of Law and Public Affairs, Nanjing University of Information Science & Technology, Nanjing 210044, China)

Abstract: Personal information protection policy is a general term for the text of the online platform companies' policies and measures for maintaining users' personal information, and, in accordance with existing laws and regulations, stipulating and explaining in details its acquisition, management and protection of personal information. Smart contracts, as specific code programs that cover informed consent rules and are automatically executed, can be used to implement personal information protection policies in intelligent application scenarios. China's *Personal Information Protection Law*, which has entered the implementation level, requires certain procedural mechanisms to ensure the compliance of personal information handling behavior of enterprises, and the non-intelligent nature of the existing procedural mechanisms makes it difficult to deal with the phenomenon of excessive collection and abuse caused by personal information handlers with technical advantages. Therefore, it is necessary to attempt to use the technical management function of smart contracts to make up the deficiency of personal information protection policy. And specific measures include targeted transformation of block-chain as bottom technology of smart contracts to meet the needs of protecting personal information so as to execute the fulfilment of the simulation of personalizing smart contracts as well as dynamic control on peculiar securing and notifying the agreement of the rules. The smart contract is embedded in the whole process of handling personal information by the online platform companies, and the personal information protection policy between the user and the platform is built with the smart contract as the core.

Key Words: smart contracts; online platform companies; personal information protection policies

[编辑: 苏慧]