文章编号:2096 - 1901(2023)04 - 0080 - 10

合规科技在数据合规中的应用价值

傅晴晴

(中国人民公安大学 法学系,北京 100038)

摘 要:政府强数据监管模式的开启,推动企业以信息技术为手段提升数据合规水平。合规科技实现数据合规治理的自动化、智能化、高效化,颠覆了企业数据合规的惯常逻辑和传统路径。以区块链技术、机器学习、隐私计算为代表的前沿数据合规科技已然成为企业部署合规思路的关键工具,信息技术及其集成价值在数据合规治理实践中得到优势发挥。合规科技为数据隐私保护、自动监管数据处理、违规行为识别预警、数据违规事后归责等提供了有力的技术赋能。提倡企业建立合规道德文化,引导其善意使用数据合规技术,规避技术固有风险,确保始终正向推进数据合规治理。

关键词:合规科技;数据合规;数据安全;区块链

中图分类号:D922.16 **文献标识码**:A

DOI:10.13710/j.cnki.cn14-1294/g.2023.04.003

数据作为信息时代的新兴生产要素,被定义为人类经济发展的引擎。数据之所以具有价值性,关键在于其作为信息源引发的可预测性。这种可预测功能诱使企业广泛获取个体信息以供精准营销,助力政府以公众信息为基进行国家治理。大数据的泛用必然触发监管机制来维持数据交易市场过猛势头与数据主体权利保护、国家信息安全保障等多者之间的平衡。2021 年 7 月,网络安全审查办公室对滴滴等企业启动数据安全审查工作,将社会的关注点聚焦于数据安全合规的问题上。在数据强监管时代,数据合规是企业生存发展的必然选择,要求企业以保障数据全生命周期安全为前提,进行合法数据处理活动,否则将承担不利刑责。至此,数据合规就成为了数据主体选择服务提供者的敏感点,也成为了政府监管企业经营的重要指标。政府在数据交互已为常态的现实场景下,为企业添赋数据合规的相关义务,突发的、硬性的合规义务给数据控制者制造了极大的经营压力。传统的数据处理模式和自身监管机制已经无法满足高标准的合规要求,此时具有前沿技术属性的合规技术就成为了解决数据合规困境的一剂良药。数据合规科技作为数据安全保护中的“优位者”[1],助力企业达到数据合规要求。

一、数据合规中的困境

(一)主观不愿合规

1. 数据合规的非营利性

数据合规意识与企业营利性经营思路在合规前期存在根本上的南辕北辙。首先必须要明确的是,数据合规作为一项风险预防举措,是一项本身不创造业绩或是利润的公司治理体系。根据国内代表性企业的数据合规操作模式可知,数据合规体系的整体搭建必然包括但不限于在资金、人力上做到极大投入,而这恰好与公司进行项目开发以获取商业利益的经营行为产生了资源利用

收稿日期:2022 - 11 - 19

作者简介:傅晴晴,中国人民公安大学法学系法律(法学)专业硕士研究生,研究方向:刑事诉讼法学。E - mail:1160073049@qq.com。

上的冲突。此外,企业战略性收购或是并购已经成为迅速增强市场竞争力和提高市场份额的重要手段。在收购行为具有巨大收益前景的前提预设下,即使被收购方或被并购方存在数据违规行为,甚至该收购决策背后带来的数据违规风险足以拖垮收购方本身,也不能直接撼动企业为牟利而作出收购决策的豪赌式野心。企业发展的最终目的是为了更好地利用资本实现最大化的自由现金流,为数据合规消耗大量资本或拒绝高利润投机有悖于企业发展之根本追求,为传统企业经营决策思维所排斥。

数据合规建设效果的不确定性是阻碍企业开展合规治理的关键因素。数据合规体系建设作为一项专业、系统、细致的治理工程,与企业生产经营必然存在磨合期,而处于建设过程中的数据合规体系不能保证对数据安全事故的绝对避免,甚至在与企业经营模式适配的过程中会催生数据安全事故的发生。以上种种不良后果都会使数据合规体系建设成效低于企业的心理预期或是超出预设风险而使推行数据合规方案的计划夭折。一旦企业在开展数据合规初次尝试时出现不可挽回的经济损失、声誉折损等负面影响,或是经营者认为数据合规体系建设极大地影响了企业正常的生产经营活动,企业决策者一般都会作出停止数据合规体系建设的决定,甚至取缔已有建设结果。

2. 联盟式合规意识薄弱

数据合规是国家对企业提出的无差别、覆盖式的硬性政策要求。企业之间互相借力,在数据合规领域内形成一种互助关系,实现共达数据合规的良性氛围,应当是强数据监管形势背景下的明智之举。但在具体落实过程中,各企业实体对数据合规联盟建设投入要素的比例划分存在分歧、互为商业竞争关系的行业各方具有直接巨额利益冲突等因素,瓦解了企业间构建利益共同体的初心共识,继而引发了数据合规联盟的全线崩盘。企业间存在不同资本量级的划分,各企业在数据合规治理体系建设中投入的财力、人力等资源必然不可能等同,那么如何让各企业认定其在数据合规联盟中的贡献符合公平原则是建立和维持合作的核心。由于存在利益分歧,在没有国家强制力强制要求企业进行数据合规联盟的前提下,实现各企业间的自愿联合可以说是天方夜谭。

数据合规标准的逐渐严苛要求企业间形成群体化的联盟协作模式,但企业间将踩界作为优胜的竞争规则,抑制合作氛围的形成。以最小的成本获取最大的利益是理性经济人所固有的本性,企业必然会按照立法设置的数据合规的最低标准进行数据处理活动,实现最低合规成本治理,这就是企业竞相的踩界行为。在此种氛围的影响下,整个地区企业的数据合规诉求基本上贴合或略高于法律最低要求这个档位。随着企业对数据价值进行另辟蹊径式的、规避合规要求的不断挖掘,全球范围内对数据合规提出了更高、更严苛的要求。企业以这种低合规水位建立的管理流程或采取的合规措施无法满足合规监管形势发展的要求。

(二)客观合规不能

1. 数据合规企业资本缺失

众所周知,日常性的数据合规管理体系搭建覆盖事前、事中、事后全周期。从企业数据合规的硬性技术设备购置到企业数据合规文化制度建设,涉及范围广、投入成本高、工程耗时大,唯有极少数的企业具备支付数据合规体系建设费用的资本和能力。对于市场占比极大的中小企业而言,即便具有数据合规意向,自身软硬件条件也无法支撑其实现预设合规目标。再加上传统的、生硬呆板的数据安全风险识别制度无法对抗算法时代数据处理的黑箱手段,原有的纯人工化的审查机制和模板化、一版式的组织架构也已不具备辨析数据违规行为的能力。可以说,现存的、未经合规治理改置的数据安全预防举措对现今“面具化”的数据违规行为而言,是形同虚设。

企业传统的数据安全把控意识区别于数据合规意识,前者倾向于识别风险目标再进行危机解

决,而后者则强调前期配置完善的日常合规管理体系实现从源头上掐断数据违规行为发生。早期的数据安全把控方案存在以下弊端:第一,纯人工式的数据违规操作识别准确性和时效性低。当数据处理违规行为仅凭数据审查员获取的初步数据和经验即可识别,那必然是该违规行为已经较大程度地脱离了数据处理的正常轨道甚至已大范围超出了违规红线,此时企业后续付出的纠正代价必然极大。第二,缺乏数据合规监管的针对性组织架构。《中华人民共和国公司法》在第二节"组织架构"中并没有为数据合规建设预留空间,大多传统公司在组织结构的设计中也极少出现独立的数据合规垂直监管形式。有些公司辩称已将合规职能并入履行监督职责的监事会或是执行企业意志的董事会,但如此附属性、非独立的合规管理模式是否能够真正落实数据合规仍有待核实。唯有合规监管层具有足够的决策独立性和决断力,才能恰当履行数据合规监管职能,并凸显数据合规对企业经营行为的决定性影响。若企业未遵从高层承诺原则[2],即董事会和执行团队未高度重视并参与合规管理之中,企业的数据合规就是一场空想。

2. 数据处理规范标准不明

数据处理规范标准模糊将极大阻碍企业数据合规治理进程。随着《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》)、《中华人民共和国网络安全法》(以下简称《网络安全法》)、《中华人民共和国数据安全法》(以下简称《数据安全法》)的陆续出台,我国形成了数据合规领域法律体系的大致框架,这将会成为企业进行数据合规的一个明确的规范标准。但是,上述规范的出台并不意味着数据合规标准规范体系的完善,仅能代表我国数据合规建设有了初步的架设,但仍无法准确甄别处在灰色模糊地带的数据处理行为。此外,当前立法给企业设定的是极原则性、笼统性的合规评判标准①,缺失对具体数据处理行为的详细判定思路或是具体的案例辅助说明,这导致企业在开展数据合规时欲进又退、踌躇不定。

域内法与域外法不衔接或冲突引发的法律适用困境也是数据合规治理开展的拦路虎。在生产要素全球化的时代背景下,数据跨境流转是不可避免的商业行为。环视全球数据合规策略可知,《通用数据保护条例》(General Data Protection Regulation,简称 GDPR)是风头极盛的立法范例。其在个人信息保护板块提出了七项数据处理基本原则,极大地引导数据控制者实现数据处理行为的合规化。但我国现有立法与 GDPR 存在概念出入②、标准冲突③等现实问题,导致国内企业数据合规不能完全参照域外范例操作。我国企业在订立有关数据处理行为的权责协议时无国内法适用意识,直接引用 GDPR 中的定义来列举合同相关方的责任和义务,以致无法对应国内法律而陷入约定不明的境地。

二、合规科技融入数据合规的价值

为实现合规前提下的数据价值创造,"数据合规科技"的概念应运而生。其理念源于欧美立法者广泛推崇的"通过设计保护隐私",被学界和实务界统一解释为一切在提供隐私保护前提下实现数据价值挖掘的应用手段。即在设计之初就将数据安全的需求嵌于其中,成为技术运作的前提,而不是出现问题之后,才将法律规则赋于其上。[3]数据合规科技的核心是利用技术实现对于监管

① 以《个人信息保护法》第二十七条作为例证,法条明文使用的"合理范围"是极模糊的立法表述,个人信息处理者对信息使用是否属于合理范围的划分方法是什么,司法裁判者极具主观色彩的评价标准是否符合立法目的等追问都属于立法空白区。

② 《数据安全法》中明文规定的"重要数据"在 GDPR 中未有规制,GDPR 中使用的"数据控制者"和"数据处理者"的定义以及相应的归责方式在我国立法中也未有可准确覆盖的术语进行替换适用。

③ GDPR 规定了数据控制者可以基于"正当利益"或"履行合同",不需经数据主体的同意即可收集和处理其个人信息,而《个人信息保护法》采取的是要求处理个人信息应当在事先充分告知的前提下取得个人同意的严格标准。二者的冲突立法极易导致企业在作出数据处理行为时被立法宽松地区迷惑,而违反立法从严地区的数据处理规范,继而被判定为数据违规。

数据的触达、辨别和获取[4],其底层逻辑是从数据处理源头实现合规规制。

(一)实现信任合规

数据合规是一项多主体间的合规合作,信息技术的参与促使非信任主体间有序释放数据合规价值。以区块链技术为例进行举证,区块链中的密码学原理、数据存储结构、共识机制三大关键机制保障其"诚实"与"透明",这也正是企业相互信任以投入合规的技术点。区块链通过技术背书建立信任机制,以算法程序来表达规则,以共识协议为本,制定可编程化的智能合约来布局整个数据存储系统,因此区块链是被各节点主体认证了的技术性可信平台。

"区块链极大的去中心化、不可篡改性、不可否认性、公开透明性共同促成了区块链作为信任基础设施的可行性,解决了参与者之间的共识问题。"[5]区块链之所以能够促成"可信协作",其根源在于以技术为名向其应用主体作出了载体可靠性的绝对保证。在庞大的数据库中,区块链能实现对各节点信息的快速复制和公开查询,企业能够实时掌握数据操作主体身份、操作轨迹和操作结果等。开源的技术基础和跨时空的溯源功能可以随时复原数据处理行为的各处细节,以此来作为后续追责的可信证据,这就打消了企业在数据合规进程中对他方以篡改、删除、增补等手段来嫁祸数据违规之责的顾虑。数据合规是信息时代发展下,社会对企业提出的新兴要求,也是企业要想持续存在必须跟从的经营主调。在政府对数据实行强监管的背景下,企业希望寻求的是一种互信的、共赢的合作关系,而非受到行业内其他主体的违规责任转嫁。信息技术所具有的"不可篡改"特性能够排除实施数据合规的主体间进行恶性谋划和算计的可能,为参与数据价值挖掘的各方消除信任壁垒,从而搭建一个以和谐互助为基础的数据合规平台,助力非信任主体间数据合规项目的有序开展。

(二)实现自动化合规

数据合规作为动态性、持续性的企业治理方案,确需自动化的合规机制引导完成数据合规监管的全流程工作。信息应用场景的动态化是大数据背景下信息技术的生命力之所在,是信息革命的价值之所在。[6]因此,数据违规行为表现形式的多样性和数据违规行为的常态化存在是数据违规行为的固有特征且无法避免。自动化数据合规审查机制保障的是对每一个数据处理行为进行监管的自主性。通过引入前沿数据合规技术赋能程序设计,实现经设计的法律保护。将数据合规审查设置为系统本能,类同于非条件放射的膝跳反应一样自觉。

区块链智能合约无需依赖任何第三方主观意志的控制,即可自动执行经各方合意达成的承诺协议。智能合约通过嵌入数据合规场景的算法来实现自动化决策,算法辅助决策具有更充分的决策基础、可容纳更大的复杂性且效率更高[7],因此借助于区块链实现的合规自动化审查的绩效表现往往优于人类决策[8]。关于数据处理是否合规的自主性审查完全是基于企业前期对数据违规行为表征作出的经验总结和结果预判。自动识别系统一旦发现符合预设特征的数据违规行为,即会进行一系列追踪、拦截等机械反应,旨在第一时间锁定目标并积极建立数据安全防线以减少损失。数据合规的自动化不仅要求在客观物理环境安全下能够进行预设的合规审查,更关注在突发情况下如何保持合规监管运行的问题。

能够让数据合规企业在区块链智能合约中设计出正确或是具有针对性的、关于数据违规行为识别条件的前提是机器学习技术,尤其是深度学习。深度学习技术在获取相当大量级的数据违规数据后,可自动提取项目特征,对数据处理行为进行建模并输出识别结果。这种建立在给定大量数据违规场景信息以实现类人脑化分析的技术层级的信息技术,具有主动调整识别模型的优势性能,也因此极好地弥补了人为设计特征造成的不完备性,较大可能地实现数据违规显性特征和隐性特征的全覆盖和全把握。

(三)实现数字孪生合规

数据合规是一项不容置疑的复杂性系统工程,这个系统工程的搭建仅仅依靠一个机制或是一种手段都无法形成有效闭环的合规安保。因此,集合各项前沿数据合规科技之智,发挥各项的突出优势,形成一个相辅相成的合规技术环即称为“数字孪生”[9]的综合技术框架,是极佳的解决思路。信息技术如何在联动模式下发挥数据合规价值呢?中国信通院发布的《隐私计算与区块链技术融合研究报告》指出,隐私计算、区块链等新兴技术的结合,可为人们提供一种在数据本身不用交换的情况下实现数据价值共享的技术路径和解决思路,在数据共享过程中实现价值挖掘与隐私保护之间的平衡。区块链技术达成去中心化共识的目的是验证数据的可信性,创造可信执行环境,并不是为了查看链上数据的原始内容;而隐私计算的目的正是在不暴露数据隐私的前提下对数据进行分析计算,二者可以说是紧密协作、完美配合的数字合规科技搭档。区块链与隐私计算相结合,可有效解决数据安全性不足的问题,使原始数据在无需出域与归集的情况下,实现多节点间的协同计算和数据隐私保护。[10]此外,机器学习与区块链技术的结合又助力创造数据合规领域最具准度的人工智能程序。去中心化的区块链为机器学习开放更加广阔的数据获取市场,链上不存在丢失值、重复或噪声的数据提高了机器学习模型的精度。从反作用来看,机器学习可以帮助区块链捕捉试图更改链上数据的节点并辅助其进行身份验证。在获取大量数据违规实例后,机器学习通过模型识别区块链上存在的数据违规操作行为并对其进行警示,以保障区块链技术的极高安全性。

隐私计算是基于隐私信息全生命周期保护的计算技术,区块链是一个分布式的数据存储系统,机器学习是人工智能技术核心。为什么区块链、机器学习结合隐私计算技术将成为各行业数据流通的标配,其要点在于三者的相辅融合为数据要素市场化提供了数据流通下的隐私保护和合规保障。数据流转的经济利益追求直接影响主体对隐私的排他性控制和支配[11],隐私计算为数据收集、整合、建模提供隐私保障,区块链解决隐私计算自身信任问题,机器学习总结数据违规事件特征识别违规风险并提供预警,三者共建起实现数据协作方身份互信、数据可信、风险把控的兼容模式,也因此形成了体系化、系统化的以信息技术集合为核心的数据合规监管机制。在政府鼓励挖掘数据价值又强监管数据合规的复杂环境下,区块链技术、隐私计算、机器学习等合规科技集合为数据要素的融合流通提供了一种可能的合规“技术解”,推动价值创造从数据向更高尖精的算法进行转移和突破。

三、融入方案

随着信息技术的不断发展,将区块链、机器学习、隐私计算等高水平科技手段引入数据合规中是创新的治理手段,也是应对政府数据合规强监管的必然选择。不论合规技术设计初衷的主要指向领域是什么,它都代表了“自动化和精简监管流程”的趋势。明确将区块链纳入数据管理战略为信息技术合规的第一步,以区块链作为基础技术铺垫科技合规思路,继而制定长期运行的多技术融入的数据合规路径。形成自动化、智能化、体系化的数据合规体系模式是企业开展合规治理的核心目标,因此引入数据合规科技作为识别数据违规行为及其后续补救方案生成的工具是明智的商业决策。

(一)“区块链”搭建合规框架

区块链技术是现今数据产业的热点,已发展成为一个内涵丰富的信息技术应用集合体[12],为数据作为生产要素市场化配置提供基础设备[13]。区块链技术赋能数据合规治理的可行性在于其自身集结的三大核心机制能使企业的数据处理行为始终处于合规的轨道内而不发生偏移。在数

据安全存储方面,企业借助区块链技术去中心化的第三平台特征和改进的加密算法,获得可自主自助存储的数据板块。在区块上,数据以链接存证或是隐私存证的形式得以展现,避免了区块链数据的绝对公开透明。

区块链存在私有链、公有链和联盟链的区分,不同类型的区块链根据功能划分赋能不同的数据合规环节。在公有链上,任何人都可以查看所有上链的信息并且只需下载必要的软件即可自由加入,此类区块链就满足了政府监管企业进行数据合规治理的需要。企业在区块链上公开必要的合规治理思路及相应的具体实践,政府得以直观把握特定企业的数据合规进程和所处水平并及时提供理论指导和技术支持。在联盟链上,可由数据合规企业合意推选出来的行业合规委员作为代表享有数据验证权,合规委员按照预设门槛诚实行事,维持数据合规联盟链上的生态稳定。以产业或行业为划分标准建立联盟链,让同一行业或是同一产业的参与方在共同的基础设施上进行交易,彼此分享数据合规见解的同时相互监督,从而促进整个行业或产业整体数据合规水平的提高。相较公有链和联盟链,私有链则具有发挥其数据机密性保障的突出优势。私有区块链建立了准入规则,即规定了谁可以在经许可的环境下查看和写入区块链。私有链禁止了外部网络访问获取信息的行为,这将是企业内部进行数据合规建设信息存储的极佳选择。在私有链上,企业是区块链集中管理者,企业邀请员工作为节点加入私有链网络以管理员工在数据处理过程中的一系列操作,一方面进行实时监管,一方面用来责任溯源,将数据违规行为的责任落实到特定个人或是特定部门。

区块链在数据合规治理领域极具价值的机制莫过于其智能合约功能组件,它实现了预先设定的场景条款的自动化、高效、准确执行。只需在区块链上设定一段计算机代码,在一定条件触发下就可以获得无人为干预的、低成本的算法操作,以助力企业审查数据处理行为的合规性或进行数据合规操作,例如对超过法定存储期限的个人信息进行自主清洗、删除、去痕等。在数据泄漏追责场景中,依据区块链所记录的相关数据处理方式及相关信息运行痕迹,可以客观准确地还原数据泄漏事故经过。结合相关主体各司其职过程中存在的过错程度,充分考虑数据处理者在主观上的恶性程度和是否属于过失疏忽,公平公正地判定各相关主体的具体责任。区块链在基于杂凑算法的块链式结构基础上,采用 Merkle 树①结构存储数据交易日志、权限变更、访问记录等信息,并加盖可信时间戳,有效解决了数据泄漏事后追溯难题。区块链的可追溯性不仅为企业内部数据泄漏调查提供信息来源,也为行政机关、司法机关行使职权和民事主体向责任方进行违约或侵权诉讼提供了具有极高证明力的证据支撑。

(二)“人工智能”+“机器学习”=数据安全警察

机器学习在获得大量违规实例数据灌输后,得以形成数据违规预测模型,代替传统的符号推理等方式,能够较高精度地识别数据违规处理行为。机器学习模型遵循算法逻辑,从大数据的具体样例中“温故而知新”出足以指导实践的普遍规则。[14]数据合规治理体系中构建的数据违规识别器就是机器学习程序,企业向其提供训练实例,给定属于违规处理数据的例子和普通合规处理数据的例子,由其进行自主学习并总结违规数据处理行为特征,继而导出相应的识别经验或是方法。挖掘出纯人工所难以发现的数据违规行为存在的关联性或是发展演化过程中的新趋势,从而更深刻地理解数据合规目标问题。

在机器学习技术的赋能下,数据合规治理体系得以建立起较为成熟的风险管理模式。其具备

① Merkle 树是一种哈希二叉树,由一个根节点、一组中间节点和一组叶节点组成。Merkle 树是区块链技术的基本组成部分,是由不同数据块的散列组成的数学数据结构,用作块中所有交易的摘要。它允许对大量数据中的内容进行有效和安全的验证,因此此结构有助于验证数据的一致性和内容的完整性。

极强的大体量数据分析能力和精准的预测警报能力实现了从数据违规实例输入到特定行为合规性审查结果输出的跨度转变。机器学习之所以在数据合规中占据有不可忽视的一席之地,关键在于深度学习能够自动提取违规实例中体现的共性特征并导出以具有复杂感知和理解能力的合规方案,不断实现模型优化以形成成熟模型并最终找到最优解。[15]基于机器学习技术的数据违规行为过滤器具有相当的能动性,具体体现为能够在违规数据处理行为发生升级进化而改变原有特征时,不需人工进行干预就灵活地调整前期识别经验,即可针对变化的违规目标对象总结新的识别规则。机器学习系统可以适应新的数据,在波动的环境中适应性地搭建任务思路,其对海量数据和合规复杂问题的洞察力丝毫不逊色于人类自身。在数据合规应用中,机器学习的行为逻辑已经完全达到了类人类思维的程度,且效率更高、精度更准。

基于机器学习技术的数据违规风险匹配机制助力企业经营满足数据权利保障合规的基础需求。企业开展经营活动而访问用户数据时需保障用户知情权,因此向其通告实施数据处理行为的具体内容是必要前置程序,包括该业务所需收集的隐私数据范围、使用方式、保存方式和期限及后续的数据删除程度等细节。根据现实经验,用户对晦涩技术语言存在理解鸿沟,机器语言的表达无法保障用户理解相关隐私风险的后果。为了平衡数据应用机器语言式表达与用户平实文字理解力之间的差距,简化用户理解成本且规避企业被误判为数据违规的裁判风险,企业采用机器学习技术对须经数据访问通告的信息进行自动化分类①。利用用户体现和人机交互技术,对用户理解力进行测评或记录相关数据。由机器学习吸收评测数据并作出相应模型,对差异化的数据访问内容进行分类,从而形成符合用户理解水平的数据访问通告,规避数据处理违规行为。

(三)隐私计算赋能数据安全流动

隐私计算技术与区块链密码学原理相结合,形成牢靠的数据机密保护层,双重保障企业数据的保密性。在数据本身底层价值井喷的现实背景下,数据开放、共享是其被高效利用以创造价值的必经之路,但保护数据隐私性是企业落实数据合规所必须达到的标准。为了迎合国家对数据的严监管要求,隐私计算作为"硬 PET(privacy - enhancing technologies,隐私增强技术)"[16]的典型,将公平信息实践原则直接嵌入信息技术的设立和运行中,利用技术代码的力量来保护隐私。其以复杂技术降低错误信任第三方的风险,背负着成为当下数据流通合规化的技术使命。隐私计算之所以在数据合规中占有一席之地,在于其作为隐私增强技术所兼有的商业价值和合规价值,在为企业节约保护数据成本和增强用户信任的同时,减少承担法律责任的风险。

隐私计算实现的是数据的"可用不可见"和"相见不相识",以同态加密为核心技术创设算法模型,算法模型为原始数据搭建起了数字加密桥梁,输入的原始数据在不可逆算法模型的加工下输出加密结果。在上述工作逻辑上,隐私计算在有效解决数据孤岛效应的同时创造了数据安全时代的新蓝海,主要体现在以下三个方面:第一,隐私计算下的数据属于在密码学原理加持下的不可逆向推导的密文,通过算法模型计算后导出的数据属于已折损的信息,极大地保障了原始数据的机密性。第二,数据的"可用不可见"能够有效防止数据滥用。只要保证决定可信执行环境的代码是按照最小必要原则进行设计的,那么基于可信执行环境的数据使用方案也是可控的。加上唯有获得授权方可进行数据使用的合意约定,数据共享将会顺其自然地符合《个人信息保护法》关于数据合规的原则要求。第三,隐私计算在一定程度上规避了数据需经告知并获授权同意使用的合规风险点。告知同意原则是指信息业者在收集个人信息之时,应当对信息主体就有关个人信息被收集、处理和利用的情况进行充分告知,并征得信息主体明确同意的原则。[17]该原则源于人的信息自

① 例如对关于隐私数据采集范围的表述采用列举式表达,充分举例说明会收集的数据类型;对获取数据的保存期的解释采用公式化表达,清晰呈现截止日期的计算方式等等。

决权[18],即立法者承认每个人具有决定自己个人信息使用方式的权利。但需注意的是,此处的个人信息所指的,应当是可以明确指向特定人的可识别信息,而排除了匿名化处理后的信息。那是否可以理解为,被隐私计算加密过的密文已经摆脱原始数据所具有个人信息属性而不需经数据主体同意授权即可使用。因此,数据处理者在收集、整合、分析被隐私计算经手过的数据时可以适当性地省略获授权的环节。隐私计算之所以能够弥合数据价值和隐私安全存在的二元对立,是因为其能够在保证不泄露原始数据的前提下支持对数据分析计算的行为,这种实现数据"可用不可见"的新兴技术手段达成了数据安全性与价值闭环。

(四)监管合规技术良善性

正确认识数据合规科技的正负面形象是善良运用的前提,只有深入把握其本身固有风险才能在适用过程中注意预防。信息技术在便利人类生产生活的同时,也形成了"独立于人类的异化力量"[19]。区块链、机器学习、隐私计算等前沿合规科技不可避免地存在客观短板或是人为主观植入的技术缺憾,且该缺陷在特定条件触发下极易产生负面价值。数据合规技术具备颠覆性重构算法应用流程的潜力,且风险不容小觑。

算法是决定数据合规科技运行逻辑的内置本源,规范算法使之符合解释权和透明性原则以实现算法合规,是引导数据合规科技良善的关键所在。在算法社会中,算法解释权是保障和尊重个体自治性的首道屏障,是机器学习和数据科学领域伦理规范的核心要素,被视为算法时代对抗数据个体的主体性和自治性沦陷和丧失的"内在之善"。[20]算法透明经常被视为解决算法黑箱问题最直接、有效的方式[21],其核心在于要求算法控制者披露源代码或者披露算法从输入到输出的基本逻辑。算法不予公开、不接受质询、不提供解释、不进行救济,难免会有演化为"算法霸权"的风险。算法黑箱,特别是那些深度学习算法以及模块化算法[22],在表象上呈现为算法共谋带来的垄断[23]、算法歧视导致的侵权[24]等,但在根本上很难让人洞悉其背后的利益机制。算法黑箱的存在为运营者提供了规避法律和监管的便利,所以会出现利用算法掩盖传统商业行为的情况[25],算法黑箱在极大程度上加剧了算法辅助决策的风险。算法辅助决策风险攀升的本质是人越来越不可能掌握决策的依据信息和逻辑方法,也越来越不可能有足够的精力参与到决策过程中去。规制算法黑箱的关键,是保持算法运作封闭性同时促成其与法律系统的相互沟通。政府作为进行数据合规强监管的主导者,应当领头建立数据合规科技的专门性合规标准,以算法标准出发,从算法解释性和算法透明两个角度出发,有效结合价值层面与技术层面的要求,为数据合规科技的算法设计提供指引。[26]

数据合规科技善良与否的决定权很大程度保有在使用者手中,其在大多数场景下仅仅处于工具的角色定位,是企业等主体作为表达数据合规意志的介质。数据合规科技通常是按照一个使用者制定的基本假设来完成所有预设工作的,确保企业做数据合规治理应当为的行为。然而谁来决定企业应该怎样落实数据合规具体标准呢,是企业自身还是政府?答案是,一个是由企业文化决定的,也即为企业决策层的基调,另一个就是由行政部门或政府机构强加给企业的法定义务决定的,且这些义务是由不断变化、存在地区差异的法律法规决定的。[27]数据合规不是公司同意的经营策略,而是被政府和立法要求的经营方针。[28]基于理性经济人的观点,获利才是企业开展经营的真实目的。数据合规科技在后续的发展过程中将会实现从赋能企业达成数据合规的善性工具向规避政府合规监管的恶性手段转变。我们必须承认,数据合规科技的演化趋势就是寻求自动计算精确的资本配置,以通过政府监管测试,同时实现回报最大化。[29]在这种被动合规的主观状态下,企业必须要建立道德文化来夯实数据合规意志,从道德自控层面来禁止实施数据处理违规行为。这一点在《美国量刑指南》中也得到逻辑论证,该准则规定"为了开展有效合规且道德的项目,企业应

该推动形成一个鼓励道德行为和承诺遵守法律的企业文化”。

四、结语

算法是数据合规科技发挥效能的核心语言,如何实现算法的可信控制,既是技术社群试图从技术理性的角度解决的现实任务[30],也是法律人需要从制度理性的角度回应的时代命题。参考区块链“以链治链”[31]的规制逻辑,尝试“以技治技”。从数据合规技术本身出发,对算法进行伦理规制和定性测评,形成规制其发展的整体思路,实现信息技术内部闭环合规纠正。在法治层面,如何构建反制“反合规技术”的法律框架也是数据合规领域的热点课题,有待学者进行进一步探究解惑。但就像“风险社会是现代性的自反性后果”这一经典命题所揭示,用以防控科技风险的法律有时恰恰是风险生产的诱因,因此寻找数据合规科技的技术与法治并行的规制路径才是正确之道。增强数据合规技术本身的可靠性、稳定性等绩效表现[32],并通过法律、行业规范、技术伦理等制度创建可信的治理环境,形成可信数据合规科技。

参考文献:

[1] 许可. 个人信息治理的科技之维[J]. 东方法学,2021(5):57 - 68.

[2] 陈瑞华. 有效合规管理的两种模式[J]. 法制与社会发展,2022,28(1):5 - 24.

[3] RUBENSTEIN I S,GOOD N. Privacy by Design:A Counterfactual Analysis of Google and Facebook Privacy Incidents [J]. Berkeley Technology Law Journal,2013,28(2):1333 - 1414.

[4] 黄尹旭. 区块链应用技术的金融市场基础设施之治理——以数字货币为例[J]. 东方法学,2020(5):56 - 65.

[5] 徐恪,李沁. 算法统治世界——智能经济的隐形秩序[M]. 北京:清华大学出版社,2017:311.

[6] 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.

[7] 于霄. 算法辅助决策中意思自治的重构[J]. 东方法学,2022(3):33 - 42.

[8] 西尔弗,张新,朱辰辰. 信号与噪音[M]. 北京:中信出版社,2013:236.

[9] 衣俊霖. 数字孪生时代的法律与问责——通过技术标准透视算法黑箱[J]. 东方法学,2021(4):77 - 92.

[10] 马明亮. “区域链 + 隐私计算”实现大数据协同办案的新技术路径[J]. 中国审判,2021(23):92 - 95.

[11] 任颖. 数字时代隐私权保护的法理构造与规则重塑[J]. 东方法学,2022(2):188 - 200.

[12] 苏宇. 区块链治理的政府责任[J]. 法商研究,2020,37(4):59 - 72.

[13] 杨东. 论反垄断法的重构:应对数字经济的挑战[J]. 中国法学,2020(3):206 - 222.

[14] 唐林垚. 数据合规科技的风险规制及法理构建[J]. 东方法学,2022(1):79 - 93.

[15] COFONE I N. Algorithmic Discrimination Is an Information Problem[J]. Hastings Law Journal,2019,70(6):1389 - 1444.

[16] BORKING J J,VERHAAR P,ECK B,et al. Handbook of Privacy and Privacy - Enhancing Technologies the Case of Intelligent Software Agents[M]. The Hague:College Bescherming Persoonsgegevens,2003:1241 - 1253.

[17] 齐爱民. 信息法原论[M]. 武汉:武汉大学出版社,2010:76.

[18] 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(2):61 - 68.

[19] 王成. 个人信息民法保护的模式选择[J]. 中国社会科学,2019(6):124 - 146,207.

[20] 陈璞. 论网络法权构建中的主体性原则[J]. 中国法学,2018(3):71 - 88.

[21] 汪庆华. 算法透明的多重维度和算法问责[J]. 比较法研究,2020(6):163 - 173.

[22] DIJKSTRA E W. The Structure of the "the" Multiprogramming System[J]. Commu Acm,1968,11(5):341 - 346.

[23] 周围. 算法共谋的反垄断法规制[J]. 法学,2020(1):40 - 59.

[24] 郑智航,徐昭曦. 大数据时代算法歧视的法律规制与司法审查——以美国法律实践为例[J]. 比较法研究,2019(4):111 - 122.

[25] 金梦. 立法伦理与算法正义——算法主体行为的法律规制[J]. 政法论坛,2021,39(1):29 - 40.

[26] 苏宇.算法规制的谱系[J].中国法学,2020(3):165 - 184.
[27] CHAFFEE E C. Creating Compliance:Exploring a Maturing Industry[J]. University of Toledo Law Review,2017,48(3):429 - 436.
[28] PACKIN,GESLEVICH N. Regtech,Compliance and Technology Judgement Rule[J]. Chicago - Kent Law Review,2018,93(1):193 - 218.
[29] SPIEGELHALTER D. Should We Trust Algorithms? [J]. PubPub,2020(1):1 - 12.
[30] 张欣.从算法危机到算法信任:算法治理的多元方案和本土化路径[J].华东政法大学学报,2019(6):17 - 30.
[31] 赵磊.区块链技术的算法规制[J].现代法学,2020(2):108 - 120.
[32] 袁康.可信算法的法律规制[J].东方法学,2021(3):5 - 21.

Application Value of Compliance Technology in Data Compliance

FU Qing - qing

(*Depatment of Law*, *People´s Public Security University of China*, *Beijing* 100038, *China*)

Abstract: The government launches strong data supervision mode to induce enterprises to improve data compliance level with information technology. Compliance technology make the automation, intelligentization and high efficiency of data compliance management a reality, which overturns the usual logic and traditional path of enterprise data compliance. Cutting - edge data compliance technology, like blockchain technology, machine learning and privacy computing, has become crucial for enterprises to deploy compliance ideas. The independent or collective value of information technology is brought into play in the practice of data compliance governance. Compliance technology provides powerful technical capabilities for data privacy protection, automatic monitoring of data processing, early warning for the identification of violations, and post - event liability for data violations. It is positive to encourage enterprises to establish a culture of compliance ethics, use data compliance technology in good faith, avoid the inherent risks of technology, and ensure reasonable data compliance governance.

Keywords: compliance technology; data compliance; data security; blockchain technology

(责任编辑:姚晓黎)