第 25 卷　第 1 期
2025 年 3 月
南京工程学院学报(社会科学版)
Journal of Nanjing Institute of Technology(Social Science Edition)
Vol. 25,No. 1
Mar. , 2025

doi:10. 13960/j. issn. 2096 - 238X. 2025. 01. 007
投稿网址:https://xb. njit. edu. cn

互联网平台数据治理的现实困境与完善路径研究

屈舒阳, 蒋恺

(云南财经大学法政学院,云南昆明,650221)

摘要:在数字化时代背景下,企业的数字化转型已成为不可逆的趋势,数据已经成为互联网平台的核心战略资源。但我国互联网平台对数据治理体系的构建还存在诸多问题:一是法律规范冗杂,形成治理"孤岛";二是企业内部体系建设不足,产生风险"暗礁";三是平台设立"霸王条款",暗含操作"黑箱"。互联网平台数据治理的制度设计应当认识到构建多元协同共治治理体系的重要性,并对现有的法律法规进行体系化的调整与修订,同时在互联网平台内部明确数据保护官的重要性与独立性,确保数据治理体系建设能够在数字时代的互联网平台中发挥其应有效能。

关键词:互联网平台;数据治理;数据保护;多元协同共治

中图分类号:D922. 29

随着"数字中国"建设的不断推进,数字经济时代的"交易大爆炸"正在逐步取代传统工业经济时代的"生产大爆炸",数字经济时代的互联网平台依靠自身所具有的优势地位在激活数据生产要素潜力、获取经济利益的同时,难免会导致对自身所保有的数据过度使用、保护不足等情况发生[1]。2024 年 8 月,国务院通过的《网络数据安全条例》旨在促进保障网络数据安全,该条例第六章"网络平台服务提供者义务"对网络平台,尤其是大型网络平台服务提供者作出了特别的义务性规定①。这表明政府也逐渐意识到大型互联网平台就如同一碰即炸的"高压炸弹",一旦发生数据泄露等事件便会对个人、社会甚至是国家造成严重危害。近年来,数据安全事件频发,国家与互联网平台都逐步意识到数据保护、数据治理的重要性,但根据每个行业独特性开展专项治理的外部法律引导和内发动力明显不足。如互联网平台保有、处理、使用大量的数据,而互联网平台存在数据使用不规范、对用户数据过度使用等问题,这些问题都亟须相关部门在数据治理层面作出强有力的回应。《国家安全法》《网络安全法》和《数据安全法》都体现了立法者对保护国家、社会、个人信息安全的重视,且立法呈现进一步细化的趋势。三年前的"滴滴被罚"一案涉及用户数据之多、被处罚之重、影响之恶劣②也让互联网平台数据治理体系的构建备受各界关注。在数字化时代的背景下,互联网平台为抢占市场先机,瓜分"蛋糕",往往违规收集与使用用户的数据并以此实现自身利益最大化。学界对互联网平台治理的讨论大多集中在保护用户个人隐私、数据跨境流通保护、数据脱敏处理等问题上,但对建立互联网平台数据治理体系以及平台预防性治理体系的研究较为缺乏。现有的互联网平台数据治理存在哪些问题?为何要对互联网平台数据进行重点保护?应当如何全方位构建互联网平台数据治理体系?基于这些问题,本文将从互联网平台数据治理的现实困境入手,基于数据治理发展的现状,分析产生这些问题的根源,最后根据现有的问题和产生问题的原因在治理主体、外部规则完善和内部体系构建方面给出优化意见。另外,数据治理虽是近年来被热议的话题,但学界尚未形成统一的定义,有观点认为数据治理既包括对数据的治理,也包括利用数据进行治理[2]。由于篇幅的限制以及侧重点的不

收稿日期:2024-12-06;**修回日期**:2025-1-15
基金项目:云南省自然科学基金面上项目"云南省国有企业合规管理体系建设:理论机制与实践路径"(202401AT071311)
作者简介:屈舒阳,博士,副教授,研究方向为刑法学。
通信作者:蒋恺,硕士研究生,研究方向为刑法学和数据法学。
E-mail: jk_010110@ 163. com
引文格式:屈舒阳,蒋恺. 互联网平台数据治理的现实困境与完善路径研究[J]. 南京工程学院学报(社会科学版),2025,25(1):44 - 52.

同,本文所述的数据治理均指对数据本身进行治理。

一、现状检视:互联网平台数据治理的现实困境

在大数据时代,数据治理成为维护平台数据安全和保护用户个人信息的关键。然而,我国在互联网平台数据治理方面存在法律规范分散、治理体系不完善和网络服务合同中存在“霸王条款”等问题。在法律层面上,权责不清导致难以形成有效的治理合力;在企业层面上,数据治理体系建设不足,增加了数据泄露风险;在用户层面上,不合理的网络服务合同和算法处理的“黑箱”操作,损害了用户权益。这些问题共同构成了数据治理的挑战与现实困境。

(一)法律规范冗杂,形成治理“孤岛”

政府、社会、企业、用户在互联网平台数据治理体系中的权责不清,难以满足数据治理的现实需求。我国法律中关于保护数据的条文基本分散在《数据安全法》《个人信息保护法》以及《网络安全法》之中,2021 年通过的《数据安全法》与《个人信息保护法》通常被认为是对 2017 年实施的《网络安全法》中的内容所作出的具体细化规定[3]。但在互联网平台数据治理的规范层面,无论是法律还是其他规范性文件,都将规定互联网平台应当承担哪些义务作为设定的重点,并没有将政府、社会、企业、用户看作数据治理的“共治”主体,使各个主体之间在治理体系中相割裂,难以形成治理合力,成为治理“孤岛”。

相关法律和规范性文件的梳理如表 1 所示。我们可以看出互联网平台数据治理的理念已经成为立法者的共识,但仍存在着一些问题。例如,《数据安全法》与《网络安全法》虽然都蕴含了建立互联网平台数据治理体系的理念,但立法者在这两部法律中均没有作出关于建立数据治理体系的具体实施方案。互联网平台数据治理体系尚缺乏纲领性的指导依据。立法者在《个人信息保护法》中规定了一些在个人数据保护层面具体可行的方案,但这些方案大多针对互联网平台作出,并未考虑个人、社会团体以及政府在数据治理中也应当发挥其重要的作用,一味对企业进行限制并不能构建行之有效的治理格局,反而会使数据治理体系的建设面临困境。同时,数据保护的外延大于个人信息保护,个人信息保护只是诸多数据要素的一部分,将互联网平台数据治理限定在个人信息保护上是片面的,并没有将数据治理作为一个整体性的概念加以考量。

表 1　现行关于数据治理有关法律、规范性文件

法律规范	立法目的	数据治理有关条文	效力层级
《网络安全法》	为了保障网络安全,维护网络空间主权和国家安全、社会公共利益,保护公民、法人和其他组织的合法权益,促进经济社会信息化健康发展,制定本法。	第二十一条　国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求,履行下列安全保护义务,保障网络免受干扰、破坏或者未经授权的访问,防止网络数据泄露或者被窃取、篡改:(一)制定内部安全管理制度和操作规程,确定网络安全负责人,落实网络安全保护责任……(四)采取数据分类、重要数据备份和加密等措施。	法律
《数据安全法》	为了规范数据处理活动,保障数据安全,促进数据开发利用,保护个人、组织的合法权益,维护国家主权、安全和发展利益,制定本法。	第四条　维护数据安全,应当坚持总体国家安全观,建立健全数据安全治理体系,提高数据安全保障能力。 第十一条　国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作,参与数据安全相关国际规则和标准的制定,促进数据跨境安全、自由流动。	法律
《个人信息保护法》	为了保护个人信息权益,规范个人信息处理活动,促进个人信息合理利用,根据宪法,制定本法。	第五十八条　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,应当履行下列义务:(一)按照国家规定建立健全个人信息保护合规制度体系……(四)定期发布个人信息保护社会责任报告,接受社会监督。	法律

续表 1

法律规范	立法目的	数据治理有关条文	效力层级
《互联网个人信息安全保护指南》	为深入贯彻落实《网络安全法》,指导个人信息持有者建立健全公民个人信息安全保护管理制度和技术措施,有效防范侵犯公民个人信息的违法行为,保障网络数据安全和公民合法权益。	6.1 收集个人信息的收集行为应满足以下要求:a) 个人信息收集前,应当遵循合法、正当、必要的原则向被收集的个人信息主体公开收集、使用规则,明示收集、使用信息的目的、方式和范围等信息;b) 个人信息收集应获得个人信息主体的同意和授权,不应收集与其提供的服务无关的个人信息,不应通过捆绑产品或服务各项业务功能等方式强迫收集个人信息……收集个人信息的系统应落实网络安全等级保护要求。	规范性文件
《网络数据安全条例》	为规范网络数据处理活动,保障网络数据安全,促进网络数据依法合理有效利用,保护个人、组织的合法权益,维护国家安全和公共利益。	第四十四条 大型网络平台服务提供者应当每年度发布个人信息保护社会责任报告,报告内容包括但不限于个人信息保护措施和成效、个人行使权利的申请受理情况、主要由外部成员组成的个人信息保护监督机构履行职责情况等。 第四十五条 大型网络平台服务提供者跨境提供网络数据,应当遵守国家数据跨境安全管理要求,健全相关技术和管理措施,防范网络数据跨境安全风险。	规范性文件

此外,部门规范性文件及其发布的各类指南也规定关于数据治理的相关内容。例如,2019 年公安部发布的《互联网个人信息安全保护指南》对数据的收集、使用、处理、审计等方面都有着具体的规定,通常也被视为数据治理体系建立的重要依据之一。全国信息安全标准化技术委员会在 2023 年印发的《网络安全标准实践指南——网络数据安全风险评估实施指引》就明确规定,对个人信息处理活动进行合规审计以及数据处理者自行开展数据安全风险评估时可组织合规部门参加。2025 年 1 月实施的《网络数据安全条例》对互联网平台数据治理提供了更加细化的要求,明确互联网平台在处理重要数据时应当设立数据安全负责人以及数据安全管理机构。虽然以上规定对互联网平台数据治理进行了细化,但大多规定片面地将互联网平台数据保护限定在了个人信息类型的数据保护上,忽视了平台本身自有的数据、运营活动中所收集的数据,同时这些规范设置大多针对互联网平台,并没有设计多方治理的有效治理体系,效力层级普遍较低,且缺乏全局意识,难以形成治理合力,不仅增加了互联网平台数据治理体系建立的难度,也导致了政府对数据进行系统性保护的治理目标的落空。

(二)体系建设不足,产生风险“暗礁”

截至 2024 年,我国共有 53 家从事信息传输、软件和信息技术服务业③的公司(下文简称“互联网相关的上市公司”)在沪深交易所挂牌上市。由于数据治理的兴起时间较短,本文通过国泰安 CSMAR 数据库的“数据中心—公告模块”对设立在我国境内并在沪深交易所挂牌上市的 53 家与互联网相关的上市公司近三年的年报进行了收集,并以“数据治理委员会”“ISO”“数据安全保护官”等为关键词对下载的年报进行了检索。本文对 53 家互联网相关的上市公司 2021—2023 年度报告中的数据治理体系建设占比④、获得 ISO 认证占比⑤、设置数据安全保护官占比⑥进行统计,得出以下数据,如图 1 所示。

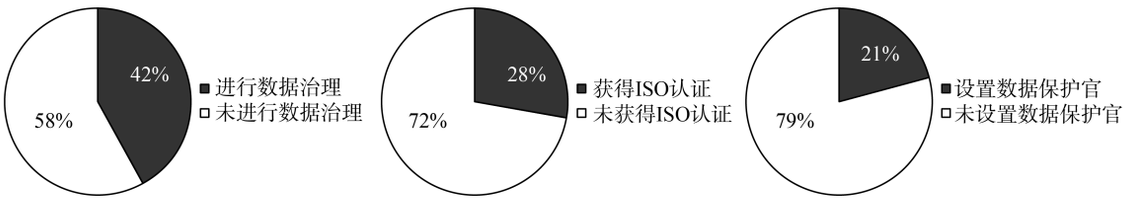

图 1 互联网相关公司数据治理现状

对 53 家互联网相关上市公司的研究发现,截至 2023 年 12 月,有 22 家互联网相关的上市公司进行了数据治理体系的专项构建工作或将数据治理放在重要的战略地位上,仅仅占总比例的 42%;而

在构建数据治理体系方面取得了一定的成效并且已获得 ISO 信息安全、隐私管理类认证的互联网相关的上市公司仅有 15 家,占到总数的 28%;仅有 11 家互联网相关的上市公司设立了首席数据保护官、信息保护官等岗位,占总数的 21%;同时具备以上三种要素⑦、在形式上建立了较为完备的数据治理体系的公司仅有 4 家,占总数的 7.5%。

数据泄露的风险不仅来自平台外部,同样也来自平台内部,平台缺乏有效的数据治理体系会使平台对内部员工的行为缺乏有效的管控,从而加剧数据泄露的风险。数据作为平台运营的生命线,贯穿了互联网平台运营的全过程,并且数据还具有可复制性、易保存性、高传输性等特点,导致用户数据的收集、处理、保存、使用等环节存在较大的泄露风险。互联网平台直接负责处理数据的工作人员能够直接接触到大量的数据,甚至绝大多数的互联网平台工作人员都能够直接或间接地接触到各类数据。而平台管理层无法事无巨细地监管每名员工的行为,同时平台又缺乏有效的数据治理手段,加剧了非法收集、处理、保存、使用数据的危险,存在损害用户权益和公司利益的高度风险。例如,经过调查发现,去年特斯拉发生的一起数据泄露事件是“内部不法行为”造成的后果,共泄露 100 GB 的数据,包括超过十万个离职和在职员工的个人信息、两千余起客户反馈特斯拉突然加速的投诉资料等一系列内部资料⑧。互联网平台内部体系的不完善,也会为下游犯罪提供便利条件。近年来,我国严打的电信网络诈骗类犯罪就以非法获取个人信息数据作为犯罪的前提与基础[4]。犯罪分子想方设法获取大量的个人信息数据以便后续开展犯罪活动。数据泄露的安全隐患不仅来源于平台外部黑客“窃取”,平台内部员工的行为对数据安全也会有极大影响,一旦掌握大量数据的互联网平台发生数据泄露事件,数据又流入不法分子手中,将会给个人、企业以及国家埋下严重的隐患。

(三)设立“霸王条款”,暗含操作“黑箱”

根据国家统计局的数据,截至 2023 年 12 月 31 日,我国互联网普及率达 77.5%,网民规模达 10.92 亿人⑨。若将婴幼儿等特殊群体排除在外,未来互联网普及率还会上升,当今社会的绝大多数人已经与互联网密不可分,使用互联网便意味着享受各类互联网平台所提供的服务,而享受服务的同时也意味着要接受互联网平台的网络服务合同。网络服务合同实质上是一种“私立规则”,“私立规则”是由互联网平台直接设定的格式条款,并没有与使用服务的具体用户进行协商,难免会出现互联网平台着重考虑自身利益而减损用户权益的情况[5]。用户相较于互联网平台处于一种天然的弱势地位,当用户拒绝互联网平台所提出的条款时,互联网平台就可能会限制用户的使用权限,甚至直接拒绝向该用户提供服务,导致了所谓的网络服务合同在一定程度上已成“霸王条款”。而用户本身就对网络服务有强烈需求,往往会忽视掉互联网平台所提供的网络服务合同中有失偏颇的条款或者不经阅读直接同意平台的网络服务合同,将各类数据授权给互联网平台使用与处理。

而在对数据处理时,算法的应用会给算法的部署者和平台的运行者带来客观的经济效益,平台的管理者会更倾向于将收集到的数据交由算法进行处理,在经济效益面前,互联网平台会更倾向于放任“黑箱”的存在并任由其发展[6]。但现行的法律并不能对算法的有效性进行规制,行政机关也缺乏对算法合法性审查的条件与能力[7]。而具有审查能力的互联网平台对于自身数据治理体系的建设又不重视,造成了在数据收集端的规则设定不合理,也造成了平台对所收集的数据存在算法处理上的“黑箱”,出现行政机关“鞭长莫及”而平台“自治”又无法发挥效用的困境。

二、症结剖析:互联网平台数据治理困境的根源

在互联网平台数据治理中,长期存在着两大核心矛盾:一是数据治理的统一性与数据利用的差异性之间的冲突,二是企业内部逐利性与数据治理公益性的矛盾。不同互联网平台因其服务性质和规模的不同,在数据收集和利用上存在显著差异,这要求数据治理规则既要统一又要具有灵活性,以适应不同平台的特定需求。此外,互联网平台的盈利模式往往依赖用户数据的收集和分析,这与数据治理的限制性措施以及保护用户隐私和公共利益之间存在天然的矛盾。

(一)数据治理统一性与数据利用差异性的冲突

制定统一的数据治理的具体文件固然是当前所需要解决的首要问题,但从现有情况来看,当前已经存在的关于数据治理体系建立的规则并没有充分考虑不同互联网平台数据利用的差异,法律规范中的考量差异性明显不足。互联网平台盈利模式的不同导致了各类平台之间数据收集的侧重点也各不相同,引发了治理规则的统一性与数据利用

差异性之间的冲突。

例如,微信、Facebook 等社交软件的数据来源主要依靠用户主动提供和社交关系的采集,用户在注册社交平台账号、发布动态内容和参与平台活动时都会向平台提供有关个人信息的数据,社交平台还可以通过分析用户的好友关系、互动行为等来优化信息流的展示。而像滴滴、Uber 等打车平台并不注重采集用户的个人数据或社交信息,这些打车平台主要通过 GPS 定位、获取 IP 地址等方式采集用户的地理位置信息以用来更好地提供服务和分析用户的需求,还能连接下游产业链,如出行后的住宿服务、行李搬运服务等。由此可见,每类互联网平台收集的数据都各有侧重,平台收集的用户数据与其服务领域紧密相关,其收集的根本原因是为了平台自身实现更好的发展,而平台收集的数据若与提供的服务明显无关,也会使平台被审查的风险大大增加,因此平台无论是从自身发展需要还是从降低自身风险出发,都决定了其收集用户的数据存在较大差异。统一的数据治理体系的构建无法考虑到每类互联网平台数据利用的差异性,若采用具体的限制标准必须根据每类互联网平台所提供的服务作出差异化的规定,对社交类互联网平台应当严格限制如位置信息数据、用户行为跟踪等数据收集方式,但对于打车平台则应当放宽位置信息数据收集,严格限制用户个人数据采集、社交关系数据采集等数据采集行为。这样不仅不会限制互联网平台的发展,又能在数据类别上有效避免互联网平台对数据的过度采集,达到保护数据的最终目的。

不同规模互联网平台采取的数据治理策略应当也采用差异化的规制模式。Furman 在其受英国财政部委托制作的报告中指出,小型互联网平台为了实现数据治理目标而承担了过重的负担,数据治理监督和审查的焦点应当更加集中在具有“战略市场地位”的大型互联网平台上,因为这些互联网平台掌握着市场的门户以及在一定程度上控制了其他平台的准入[8]。保护小型互联网平台并不要求政府必须在原有数据保护的要求下放宽对其的监管,无论大型或小型互联网平台都需要有统一的数据治理规则去引导该体系的构建,应在统一的框架体系下根据互联网平台的规模和数据利用的差异性去实施差异化的审查和监督措施。但不可否认的是,大型互联网平台收集了更多用户的数据,其威胁公共利益的风险也远远大于小型互联网平台,因此,大型互联网平台应当建立更加严格的数据治理体系,有关部门也应当投入更多的精力对这些大型互联网平台的数据治理体系进行审查。

综上,互联网平台对于自身服务定位不同,导致了收集用户数据的类型和程度存在差异;平台规模和发展程度也不同,导致平台存在的潜在威胁各不相同。这些因素共同导致了治理制度统一性与数据利用差异性的冲突。

(二)企业内部逐利性与数据治理公益性的矛盾

数据是互联网平台重要的生产要素之一,早期的互联网平台提供的基础服务以免费服务为主,用户使用互联网平台满足自身需求所支付的对价并不是金钱,而是数据[9]。用户的数据被互联网平台收集并分析,再向广告商出租广告位并利用数据对每个用户进行个性化分析,以此提高广告的点击量、转化率等指标,以便获得更高的收入。虽然互联网平台盈利手段早已多样化,但平台经济的现实运行方式从来都不会是一种纯粹的共赢,在使用数据的各个阶段都体现了互联网平台利用自身的技术优势对数据价值进行不断地攫取[10],同时互联网平台依靠收集、分析、处理用户数据并利用这些数据在竞争激烈的互联网行业中保持本平台的优势地位。简单来说,互联网平台依靠数据实现存续和发展。这种对数据的“天然渴望”和资本的逐利性不可避免地导致了互联网平台想尽可能多地收集用户数据。平台的这些特性导致网络服务合同屡屡出现“霸王条款”“隐形规则”“过度收集”等损害用户利益的情况。

用户对自身数据的处分权一般被视为是对个人利益的处分,但国内使用互联网的人数极为庞大,这意味着互联网平台服务的对象并不是具体的人,而是社会中不特定的多数人,当用户群体足以构成社会公众时,个人利益就上升为公共利益。基于《个人信息保护法》中的“正当”“必要”原则,公共利益要求互联网平台不能过度收集和处理用户数据,但多数网络服务合同中所设置的用户隐私条款都远远超出了“正当”“必要”的范围。

若在互联网平台中建立数据管理部门,那么管理部门所代表的公共利益就会与互联网平台内源的逐利性发生冲突。互联网平台为实现自身野蛮生长,毫无理由和根据地去获得更多的用户数据,保护公共利益的同时就会不可避免地损害到平台的产业利益,平台的内部机构之间可能出现不可调和的矛盾。如何化解公共利益和平台产业利益之间的冲突就成为建立数据治理体系需要解决的难题。

三、体系构建:互联网平台数据治理路径

互联网平台所面临的数据治理困境不仅来源于现有法律体系的不完善,也来源于数据治理本身的天然矛盾。互联网平台的数据安全不仅关乎用户个人信息安全,还对社会总体安全甚至国家安全都有重大影响。如何打破个人、企业、社会团体与国家之间的壁垒,实现科学化的数据治理格局;如何协调不同效力位阶的各类规范,构筑精细化的数据治理体系;如何处理平台逐利性与社会责任之间的矛盾,实现平台数据治理的自我控制,成为我国数据治理层面亟须解决的问题。

(一)构建多元共治的协同治理模式

互联网平台多元共治治理模式的构建主要是为了跳脱出原有的“政府—互联网平台”二元治理格局,将平台用户、第三方监管机构等主体纳入原有治理格局之中,形成多元共治、权责分明的治理格局(图 2)。

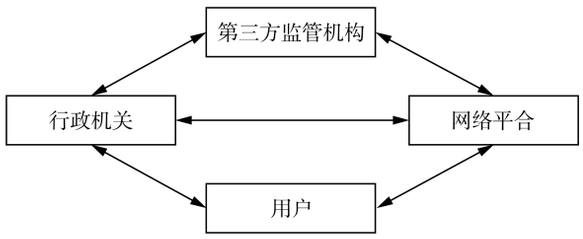

图 2　多元治理模式关系

通常意义上,在实践中运用第三方监督评估机制更接近于一种“惩罚性监管方式”,是行政机关对具有重大法律风险的企业所采取的一种特殊手段,企业也通常会将其视为负担与束缚。随着国家对数据安全重视程度的不断提高,对数据保护的要求也随之提升,越来越多的互联网平台更愿意在事前将国家监管的压力转化为自我监管的动力,“预防性监管方式”若想要落到实处,就必须跳脱出原有“惩罚性监管方式”的囹圄[11]。互联网平台对数据要素的处理、使用极大依托新兴技术,而新兴技术在数字经济的驱动下发展日新月异,因此,传统的单向静态监管难以适应数字时代的发展速度[12]。同时,立法者和执法者在数据要素中并不具备优势地位,难免存在规制手段滞后、规制效果不佳等问题[13],而第三方监管机构参与企业的监督管理已经具有了一定的实践基础。同时,国内也已经出现了大型互联网平台依托其技术优势帮助其他互联网平台保障数据安全的服务。数据治理的内部控制与外部监管的底层技术基本相同,在一些技术性的治理方案上也存在共通之处,因此,行政机关应充分考虑互联网平台所属的行业特点,健全完善行业监管、平台自治、全链监管的“预防性”数据治理体系[14]。具体而言,数据治理体系构建时应更注重“预防性监管方式”,而“预防性监管方式”要求在事前就建立有效的治理体系。第三方监管机构应当承担起对企业的数据治理情况进行调查、评估、监督和考察的职能,同时在企业内部自我控制失灵时应当及时承担“纠偏”的职能,将包容审慎监管的理念融入互联网平台的建设之中。若平台能够及时自我纠偏,第三方监管机构则没有必要将平台的轻微过错报告行政机关,应为平台经济的发展争取相对宽松的政策空间[15]。互联网平台在数据治理体系的建设之初就应接受第三方监管机构的监督与审查,第三方监管机构采用“对平台审慎、对创新包容、对数据监督”的新型监管模式,保护数据要素发展的同时大幅提升平台数据治理体系的有效性,形成“执法机关—第三方监管机构—互联网平台”三方的多元共治关系[16]。

此外,在多元共治的治理模式中,行政机关还应加强与利益相关者的交流与联系,包括但不限于与行业协会、监管机构等相关主体的联系[17]。在互联网平台为治理对象的情况下,用户是互联网平台最主要、最直接的利益相关者,用户使用互联网平台时能够最直观地感受到平台的更新和对数据获取的不同需求。例如,用户在使用 IOS 系统时,输入“这里发现石油”“我发现了石油”等相关语句,IOS 系统就会直接开启定位功能获取用户的实时定位⑩。大量用户的反映与投诉,也迫使 IOS 官方客服作出回应,尽管客服回应开启定位属于 IOS 系统的随机事件,用户的任何操作都可能使定位功能开启,但经历这场风波后,再采取相同或类似的操作并不会使系统定位功能开启。可见,用户的使用体验是互联网平台服务最直观的写照,平台出现的侵犯隐私行为往往是由用户最先发现的,互联网平台多元共治体系的构建,要重视用户的反馈与投诉并且建立相应的风险预警措施,如用户反馈的互联网平台非法获取用户位置信息等行为,一经查实,相关部门就应当立刻采取措施,禁止互联网平台获取用户位置的权限并进行调查与研判。

构建多元治理格局是将原有已经存在的“第三方监管机构”应用到数据治理体系构建之中,并利用互联网平台用户与互联网平台之间天然紧密的

联系,形成用户与行政机关之间有效的连接,使得行政机关能够通过用户的直观反馈对互联网平台进行实时监管,最终形成互联网平台数据多元共治的协同治理格局。

(二)调整外部法律法规体系

在外部法律规制层面,本文认为数据治理体系的构建应当在《数据安全法》的规范框架下,通过制定专门的下位法来实现,具体理由如下:第一,《数据安全法》为我国保护数据搭建了基本的法律框架,明确了在数据保护中各类权利义务主体,属于指引性规范,其中第四条就明确指出要建立健全数据安全治理体系,提高数据安全保障能力⑪。而无论是站在国家的视角上还是企业的视角上,互联网平台建立健全数据治理体系都是当今保护数据的关键一环。第二,用户的个人信息保护只是数据保护项下的一部分,虽《个人信息法》也有必要对数据治理进行具体规定,但针对的只是用户个人数据层面的保护,建立数据治理体系不应当仅仅针对个人信息层面,而应放眼于整个数据治理体系的构筑这一更广的层面之上。因此,数据治理体系应将《数据安全法》作为纲领性法律文件,并在《数据安全法》之下利用《条例》《办法》等下位阶法律文件对数据治理体系作出细化规定,构建出系统化、体系化的法律规范体系,这不仅符合《数据安全法》的立法精神,又能凸显国家对数据治理的极大重视。

此外,为了指导互联网平台建立数据治理体系,行政机关应发布具体可操作的数据治理指引。一方面,针对互联网平台普遍面临的数据安全风险,行政机关应当依照《信息技术—大数据—数据治理实施指南》中的制度构建,在数据治理领域,依照数据治理的总体要求,制定的综合性指引;另一方面则是要针对特殊互联网平台所面对的数据安全挑战而量身定制专门性的指引,如参与跨国数据流通的互联网平台,不仅要遵守我国的法律,同时也要符合欧盟的《通用数据保护条例》、美国的《数据隐私保护法案》等数据保护相关法律。各国的法律制度各不相同,仅仅依靠国内的法律规定建立数据治理体系可能会造成国内数据治理体系与国外数据治理相关制度相抵触,从而影响国内公司的跨国商业行为,因此,行政机关在向特殊互联网平台发布具体治理体系构建要求时需要考虑各类互联网平台的具体需求。这些指引的目的是帮助企业构建以治理目标、组织架构、运行机制和治理文化为核心的数据治理体系。同时,在数据治理指引中,行政机关应当明确数据治理体系有效的评判标准。这套标准将成为数据监管部门在对企业实施行政执法时,用以评估其数据治理体系能否有效防范风险的重要评判标准,并且也能被运用在前文所述的“预防型监管方式”以及第三方监管机构的评估中。

(三)重塑内部数据治理管理机制

一般情况下,互联网公司在股东会和董事会之下设立技术部、人事部、运营部、策划部、法务部等部门来管理公司日常运营事宜。而大多数本土互联网公司都没有设立专门的数据安全保护官。数据保护是互联网平台数据治理体系的“命脉”,极大程度关系到互联网公司前途与命运。由于我国对数据保护官的定位较为模糊,现有法律条文缺少对数据保护官明确的规定,我国本土互联网平台对数据保护官的重要地位的认识程度明显不足。我国本土互联网平台要想全面建立数据治理体系,必须要求互联网平台招聘数据安全保护官(Data Protection Officer, DPO),以全面统筹企业内部数据保护事宜,并在数据安全保护官的领导下建立一个独立的数据治理部门,该部门直接对企业的董事会和股东会负责。数据治理部门最应凸显的是其独立性,体现在两个方面:在形式上,数据治理部门不属于其他部门的附属机构,如果互联网平台本来就设有企业管理部门,那么设立的数据治理部门应当与企业管理部门平行,互不从属,在形式上凸显其独立地位和重要性;在实质上,数据治理部门的工作要独立于互联网平台其他部门的工作,在相关数据保护事宜上并不受平台董事会、股东会或其他高管的干涉并且不会因执行相关数据保护事宜而被企业解雇或在任何方面被区别对待[18]。

互联网平台数据治理体系的构建与完善需要平台自身投入较大的成本,由此会产生较重的经济负担,违反数据保护规定所带来的罚款与互联网平台设立数据安全保护官的成本也存在着利益上的矛盾[19]。小型互联网平台自身盈利能力有限,由于平台规模小,平台可能都没有形成较为完整的体系架构,若是“一刀切”地要求所有互联网平台建立数据治理体系会导致小型平台失去生存和发展的空间。因此,完善互联网平台内部的体系应当根据互联网平台的规模分别作出规定,根据平台人员和服务用户的数量将互联网平台分为大型互联网平台、中型互联网平台和小型互联网平台⑫。大型互联网平台是指服务用户数量较大并且在全国范围内都具有较大影响力的互联网平台,如一些上市互联网公司或资本雄厚的互联网平台,国家对这类互

联网平台可以采用强制性规定,要求必须严格按照法律规定独立建立数据治理体系;中型互联网平台是指已积累了一定数量的用户并且在一定区域范围内具有较大影响力的平台,国家对这类平台应当要求其在一定年限内初步完成企业内部数据治理体系的框架构建;由于小型互联网平台正处于起步阶段,人员与资金有限,自身能力与大、中型互联网平台相差较远,国家应着重区别对待。一方面,我国互联网平台众多,许多新兴互联网平台仍然在起步阶段,为保障互联网平台能在起步阶段不受到过多的限制,国家应结合具体情况对不同规模互联网平台进行区别对待和处理;另一方面,国家、社会、个人对数据保护的要求在数字化时代中更为严格,数据治理已经成为互联网平台不可绕开的议题,数据保护治理的理念应根植在平台发展初期,使数据保护行为贯穿互联网平台发展的全过程。

互联网平台应采用分段式的数据治理结构模式,可以参考借鉴欧盟实施的《通用数据保护条例》,在互联网平台治理中采取数据安全保护官共同聘任制度[20],采用多家中、小型互联网平台共同招聘一名数据安全保护官和建立一个数据治理部门的方法,这既能分摊成本,避免因互联网平台的数据治理造成过重的负担,还能够培养专业化的治理中介机构,使数据治理向专业化、体系化、领域化发展。

四、结语

在互联网技术快速发展的时代,国内外都不约而同地将互联网平台数据治理视为保护数据安全的重中之重,对数据治理不断提出新要求。我国数据治理的发展历程虽然只有短短几年,在贯彻落实数据治理体系的构建上还处于探索阶段,但国际上数据治理如火如荼,我国本土互联网平台要想加速融入国际市场,就必须在数据治理体系上与国际贸易中的其他标准形成有效衔接。构筑预防性数据治理体系既能够有效降低互联网平台出现的法律风险,又能够防患于未然,构筑企业内部对法律风险的“防火墙”,在预防互联网平台违法犯罪以及数字中国建设过程中有着极为重要的战略地位。本文从现有互联网平台存在的问题出发,分析产生问题的原因并从多元共治、外部法律制度层面和平台内部体系层面给出了优化路径,但是,多元共治体系与外部法律制度如何有效衔接,外部法律制度应当如何指导平台内部治理体系重构等问题还需进行深入研究。

注释:

①《网络数据安全条例》第四十四条　大型网络平台服务提供者应当每年度发布个人信息保护社会责任报告,报告内容包括但不限于个人信息保护措施和成效、个人行使权利的申请受理情况、主要由外部成员组成的个人信息保护监督机构履行职责情况等。

② 参见《国家互联网信息办公室对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定》,中国网信网,https://www.cac.gov.cn/2022-07/21/c_1660021534306352.htm,最后访问日期为 2025 年 1 月 13 日。

③ 选取上市公司行业划分标准为:信息传输、软件和信息技术服务业(GB/T 4754—2017)。

④ 此处数据治理体系建设是指在互联网相关上市公司的年报中,公司表示已经建立或者正在完善数据治理体系、信息保护体系,将数据治理作为企业的重要战略方向或明确要进行数据治理建设。

⑤ 此处 ISO 为 ISO 27001 的简写,ISO 27001 是一种信息安全管理体系(Information Security Management System, ISMS)标准,是世界上广泛应用的、通用及可证明的信息安全管理框架之一,旨在通过采取一系列信息安全管理制度、流程和控制措施,确保组织能够最大限度地保护其信息资产和利益。

⑥ 此处的保护官是指在互联网相关上市公司内部已经明确设立的首席合规官或者数据保护官。

⑦ 三种要素齐备是指互联网相关上市公司同时进行了数据治理体系建设、获得了 ISO 27001 信息安全体系认证以及设立了首席数据保护官。

⑧ 有“内鬼”!特斯拉 100GB 数据泄露原因查明 影响超 7.5 万人,腾讯网,https://news.qq.com/rain/a/20230822A0201T00,最后访问日期为 2024 年 11 月 21 日。

⑨ 数据来源于国家统计局,https://data.stats.gov.cn/easyquery.htm?cn=C01&zb=A0G0Z&sj=2023,最后访问日期为 2024 年 11 月 1 日。

⑩ “这里发现石油”触发定位?这里真的发现了!澎湃新闻网,https://m.thepaper.cn/user_interaction_3977389,最后访问日期为 2024 年 11 月 13 日。

⑪《数据安全法》第四条　维护数据安全,应当坚持总体国家安全观,建立健全数据安全治理体系,提高数据安全保障能力。

⑫ 大、中、小型互联网平台应当通过实证研究,结合经济学、管理学知识进行划分,划分的具体方法并不是本文的研究内容。

参考文献:

[1] 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.

[2] 沈岿.数据治理与软法[J].财经法学,2020(1):3-12.

[3] 胡玲,马忠法. 论我国企业数据合规体系的构建及其法律障碍[J]. 科技与法律(中英文),2023(2):42-51.
[4] 马丙合,马方. 中国式现代化进程中的数据风险与安全治理[J]. 重庆社会科学,2024(10):103-114.
[5] 吕炳斌. 论网络用户对"数据"的权利——兼论网络法中的产业政策和利益衡量[J]. 法律科学(西北政法大学学报),2018(6):56-66.
[6] 陈敏,孙占利. 算法"黑箱"的技术与法治耦合治理[J]. 法治论坛,2022(4):3-18.
[7] 陈姿含. 人工智能算法决策中的敏感个人信息保护[J]. 法律科学(西北政法大学学报),2024(6):63-75.
[8] Furman J, Coyle D. Unlocking digital competition: Report of the Digital Competition Expert Panel[EB/OL]. (2019-03-13)[2024-06-02]. https://assets.publishing.service.gov.uk/media/5c88150ee5274a230219c35f/unlocking_digital_competition_furman_review_web.pdf.
[9] 李勇坚,夏杰长. 数字经济背景下超级平台双轮垄断的潜在风险与防范策略[J]. 改革,2020(8):58-67.
[10] 李希梁. 互联网平台数据治理的理论意蕴与实现路径[J/OL]. 重庆大学学报(社会科学版)(2023-03-01)[2024-11-13]. https://kns.cnki.net/kcms/detail//50.1023.C.20230301.1237.002.html.
[11] 陈瑞华. 论企业合规在行政监管机制中的地位[J]. 上海政法学院学报(法治论丛),2021(6):1-20.
[12] 刘权. 数字经济视域下包容审慎监管的法治逻辑[J]. 法学研究,2022(4):37-51.
[13] 李牧. 论企业数据的行政合规[J]. 法学评论,2025,43(1):67-76.
[14] 周乾,洪晓琪. 合规科技与监管科技的协同发展[J]. 长春大学学报,2024(11):80-87.
[15] 王永强. 包容审慎监管视角下平台经济竞争失序的法治应对[J]. 法学评论,2024(2):77-87.
[16] 胡仙芝,刘海军. 包容审慎监管:论新基建监管框架构建的过渡性和开放性[J]. 管理世界,2022(2):116-128,168,8.
[17] 王小乾. 数据要素合规流通的风险评估与防范[J]. 信息通信技术与政策,2024(4):41-46.
[18] 王楠. GDPR"数据保护官"制度探析——兼论其对中国的启示[J]. 电子知识产权,2019(6):16-26.
[19] 相丽玲,王秀清. 中外数据保护官制度分析及启示[J]. 情报杂志,2021,40(6):137-142.
[20] 刘江山. 欧盟通用数据保护条例中的数据保护官制度[J]. 中国科技论坛,2019(12):173-179.

Research on the Real Dilemmas and Enhancement Strategies in Data Governance within Internet Platforms

QU Shuyang, JIANG Kai
(School of Law and Politics, Yunnan University of Finance and Economics, Kunming 650221, China)

Abstract: In the contemporary digital landscape, transformation of enterprises into data-driven entities has emerged as an inexorable trend, with data emerging as a pivotal strategic asset for internet platforms. Nevertheless, there are still numerous challenges regarding the establishment of a data governance system within China's internet ecosystem: Firstly, at the legal level, existing regulations are excessively convoluted, resulting in fragmented "islands" of governance; secondly, there is a notable deficiency in the internal system development within enterprises, leading to potential risk "reefs"; thirdly, platforms often impose "unilateral clauses," which imply opaque operational practices. In designing institutional frameworks for data governance on internet platforms, it is imperative to acknowledge the importance of establishing a collaborative multi-stakeholder governance system. This endeavor necessitates systematic adjustments and refinements to current laws and regulations. Additionally, it is vital to clarify the significance and independence of Data Protection Officers within the internet platforms' internal structures, ensuring that the development of data governance systems could effectively fulfill its intended role in this digital epoch.

Key words: internet platforms; data governance; data protection; multi-stakeholder collaborative governance