数字经济刑事合规风险的多维性分析及规制路径

热娜古·阿帕尔
(喀什大学 法政学院,新疆 喀什 844000)

摘要:在数字经济语境下,网络平台与数据要素在为企业等市场主体带来经济价值的同时,也增加了其陷入刑事法律风险的可能性。以企业参与数字经济的行为类型为切入点,探赜市场主体在网络数据安全、网络空间安全、数字知识产权以及其他主要领域可能面临的刑事合规风险,从客体维度、空间维度、法益维度进行具体展开。为提升企业应对刑事合规风险的能力,应当在理论层面以激励原则、权利义务一致原则与系统性治理原则为指导构建企业合规管理体系,在实践层面建构保护数据安全、空间安全以及数字知识产权的具体机制,并通过建设刑事合规数字平台、强化监测预警机制与监督评估机制实现多维一体的企业数字经济刑事合规风险预防,助力企业在数字经济发展过程中取得优势地位。

关键词:数字经济;数据犯罪;刑事合规;数字合规

中图分类号:D924.3 **文献标志码**:A **文章编号**:2096-028X(2024)02-0077-14

一、问题的提出

刑事合规问题目前正在理论界引起广泛讨论。在正式进入讨论之前,分清论域的时代性特征是尤为重要的,目前中国正处于数字经济的大环境中,许多刑事合规问题都与该时代背景密不可分。“十四五”期间,中国政府推出关于扶植数字经济发展的新政策,数据被明确为一种新型生产要素,由此正式开启数字经济发展的新阶段。

数字经济的刑事合规风险有别于一般意义的数字经济刑事风险。数字经济的刑事合规风险是涵摄于数字经济刑事风险概念之下的,从企业合规角度出发并对此进行分析的刑事风险。对从事数据收集和利用活动的企业来说,企业日常经营管理往往以数据为载体和依托,其经营管理活动是否合法,很大程度取决于企业数据处理活动是否合法。如果企业掌握数据优势,就很容易发生其通过违法的数据处理行为来谋取利益的情况。于是,数据行为是否合规成为审查其刑事合规的必要内容。① 面对数字经济发展及其所带来的风险挑战,刑法立法与司法已经存在滞后性,需要构建确保数字经济安全的规范新形态。

从功能主义的角度,对数字经济刑事合规的风险进行研究和讨论,能够降低企业刑事风险并最终在维护社会主义市场秩序层面起到积极的作用。一般来说,风险是指未来结果的不确定性或损失,根据风险的内容和来源的不同,可以从不同维度对风险进行界分,如有的研究者将刑事合规风险分为内部刑事合规风险、外部刑事合规风险、特别刑事合规风险;②刑事合规风险又可以根据企业及企业内部人员所承担的角色不同,细分为企业作为被害方的刑事合规风险、企业作为犯罪主体的单位犯罪刑事合规风险、企业内部人员和机构

收稿日期:2024-01-13
基金项目:新疆维吾尔自治区党委宣传部“‘天山英才’培养计划——新疆文化名家暨‘四个一批’人才”项目;2021年度喀什大学新疆中华民族多元一体格局历史与文化研究基地课题“中华民族共同体意识的法治凝练与实践路径研究”(KSJDC011)
作者简介:热娜古·阿帕尔,女,法学博士,喀什大学法政学院副教授、硕士生导师。

① 参见焦艳:《大数据时代企业应加强数据合规体系建设》,载法治网2023年2月3日,http://www.legaldaily.com.cn/sylm/content/2023-02/03/content_8819061.html。

② 参见阎丽霞:《企业刑事合规风险防控研究》,山西大学2021年硕士学位论文,第12页。

作为犯罪主体的刑事合规风险等。[①] 考虑到数字经济以数字产业化和产业数字化为关键核心,经济活动主要围绕着“数字”展开,与网络技术、信息数据息息相关,而企业往往并没有相匹配的合规意识,笔者主要从网络数据安全刑事合规风险、网络空间安全刑事合规风险、数字知识产权刑事合规风险以及其他主要的刑事合规风险,如网络服务提供者滥用市场支配地位的刑事合规风险四个面向,对数字经济下刑事合规风险进行多维性分析并提出相适应的规制路径。

二、数字经济刑事合规风险的多维面向

数字经济刑事合规需注重对其特征的分析,因其复杂性特点需进行多维性分析。在数字经济背景下,数据成为相应犯罪行为的主要侵害客体,因此需关注网络的空间性以及隐蔽性特点,建立企业数据安全和网络空间安全的事前风险防范机制以达到犯罪预防的效果。通过对于数字经济犯罪种类的类型化分析,数字知识产权类型犯罪占比较大,应在事先预防和事后规制两方面予以重点关注。风险本身就有高度的延展性,现代刑法的发展历史就不断表明,新的风险类型会持续出现或者被发现,如何有效预防、控制与分配风险成为刑法的重要任务之一。亦即,刑法不再是简单的事后惩罚,而逐渐承担起风险预防之重任。因罪刑法定原则之限制,刑法只能围绕对该法益之侵犯最严重的行为进行规制,形成构成要件。由此可见,直接对风险进行类型化一方面难以实现,即界定刑法之罪名者并非单纯的风险,而是形成该风险的最应当进行刑事处罚且相对边界固定、文意清楚的犯罪行为,换言之,刑法界定罪名应当同时兼顾形式理性和实质理性,而不能简单地因为风险本身的重大性就将其规定为犯罪。另一方面风险是不断增加的,某些风险是固有的,只是伴随着时代的发展而逐步被重视,例如伴随人民日益增长的美好生活需要而被逐渐重视的环境风险;有些风险则是新产生的,最典型的是目前网络生活中出现的各种风险。具体到数字经济来说,数字经济的蓬勃发展,不仅带来经济领域的新产业和新业态,而且带来犯罪活动的新场域;既催生出涉数字货币、网络虚拟财产、数据等新型权益的犯罪,也为传统犯罪问题带来新的认定问题。数字经济刑事合规所针对的就是伴随着数字经济发展而产生的新类型风险。对此,结合刑事法律的特性,笔者认为类型化依据应尽可能减少对风险本身的内涵界定,结合具体的场景、要件等视角进行观察是相对可行的方案。

还需要说明的是,针对被规范保护或者被犯罪侵犯的对象,中国刑法理论中同时存在“法益”和“犯罪客体”的概念,尽管在终极立场上,二者之间可能存在“水火不容”的对立关系,但是在具体个案或者场景中,二者的区分并不是那么重要。笔者对二者的区分持相对缓和的立场,将法益视为相对抽象的概念,而客体则是相对具体的法益之承载者,换言之,在本部分展开逻辑的讨论中,出现“法益”时意味着从相对形而上的角度考察规范保护目的,而出现“犯罪客体”时则是在要件式审查中,具体展开如下。

(一)数据安全刑事合规风险——客体维度

数据安全意味着保护数字数据(例如数据库中的数据)免受破坏性力量和未经授权用户的不良行为的影响,例如网络攻击或数据泄露。从概念上讲,数字经济背景下的企业发展存在两个主要特征:一是通过数据资源直接或间接地发挥引导作用,以推动生产力发展;二是跨越初级的信息处理技术和网络建设阶段,进入运用大数据、[②]区块链、人工智能等新兴技术的信息经济的高级阶段。[③] 因此可以说,数字经济发展的核心就是数据资源。不过,在以现代信息网络作为重要载体的背景下,企业在整理、应用数据资源时会面临网络数据安全刑事合规风险,从发生环节来讲,主要包括以下三个方面。

第一,数据收集的刑事合规风险。发展数字经济首先需要收集和形成数据资源,因其收集的主要对象为个人信息,若缺乏被收集信息方的知情及同意,对个人信息进行过度收集和获取,就形成了最大的法律风险。[④] 根据《中华人民共和国刑法》(简称《刑法》)和《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》的规定,如果单位以窃取或者购买等非法方式获取个人信息,情

① 参见刘建忠:《企业内部刑事合规风险防控及框架设计》,载《中国律师》2021年第4期,第63页。

② 参见孙晨霞、施羽暇:《近年来大数据技术前沿与热点研究——基于2015—2021年VOSviewer相关文献的高频术语可视化分析》,载《中国科技术语》2023年第1期,第89页。

③ 参见申雅琛:《数字经济理论与实践》,吉林人民出版社2022年版,第3-4页。

④ 参见李鹏、吴舒敏:《数据安全视角下企业刑事合规的检视与治理》,载《人民检察》2023年第7期,第23页。

节严重的,可以构成非法获取型的侵犯公民个人信息罪。实践中较为典型的表现形式有:一是未经授权擅自收集用户人脸识别、身份证号等个人信息;二是超越授权范围收集个人信息,如强制授权和过度授权。除此之外,如果单位使用网络爬虫技术收集数据,也可能涉及多种刑事犯罪:例如,攻破目标系统的反爬技术进行数据收集,可能构成非法获取计算机信息系统数据罪;如果爬虫技术对目标网页进行控制并收集数据,可能构成非法控制计算机信息系统罪。在"巧达公司侵犯公民个人信息案"中,巧达公司组建专业爬虫技术团队,在没有取得求职者本人和平台的直接授权的情况下,秘密爬取平台个人信息 2.1 亿余条,最终被判处罚金人民币四千万元。①

第二,数据使用的刑事合规风险。在信息社会中,数据毫无疑问是一种生产要素,可以反复使用并创造更有价值的资源。企业在获得信息数据后势必涉及使用信息数据并获得经济效益,而这个过程中较容易出现不当使用的问题,即数据滥用。在此环节,常见的刑事合规风险包括:一是为了企业盈利目标,违法地将收集到的信息出售、提供或共享给第三方以从中牟利,可能触犯侵犯公民个人信息罪;二是如果非法提供、出售数据的行为,帮助了他人实施信息网络犯罪活动或为其犯罪活动提供了一定程度的便利,则具备构成帮助信息网络犯罪活动罪(简称帮信罪)的可能性。在"常某、颜某侵犯公民个人信息案"中,数据堂公司将通过技术服务获取的原始非法数据出售给专门成立以售卖公民个人信息的金时公司,法院判决其应当承担刑事责任。②

第三,数据管理的刑事合规风险。数字经济带来的巨大经济利益驱动越来越多的新旧企业进入市场,其中占比较大的互联网企业已经成为数字社会的重要力量,其在提供各类服务等经营活动的过程中,不可避免地会收集、汇聚到大量的用户个人信息,如果不尽职履行数据保障义务,导致数据信息被泄露,甚至造成严重后果的,可能会面临刑事处罚,并存在构成侵犯公民个人信息罪与拒不履行信息网络安全管理义务罪数罪并罚的可能。在数字经济时代,随着财产的范围进一步扩张,大范围窃取公民信息并转移网络财产的行为可能造成盗窃罪和侵犯公民个人信息罪的竞合。在可预见的未来,由于责任分配的日益多元以及前置,立法会更加倾向于通过加重企业监管责任的方式来实现对风险的预防与治理。具体到刑事领域来说,为严密监管责任刑事法网,针对企业尤其是网络服务提供者的监管责任的罪名或将越来越多。此外,合规意味着数字经济时代的企业本身作为犯罪主体,其内部成员的不法行为也应当由企业承担一定的责任,至少是安全责任。综合来看,数据管理的刑事合规风险相对较重,遍布各个层面。

(二)网络空间安全刑事合规风险——空间维度

上文所述的数据安全刑事风险的犯罪客体为企业(或个人)的数据,犯罪主体大多为直接参与市场经济经营活动(例如外卖平台和社交平台)的企业或个人,覆盖到社会经济生活的方方面面。除考虑犯罪行为的客体特征,也需同时注意数字经济领域犯罪其他维度的特征。此处需考虑互联网的空间性特征,因为网络犯罪有别于其他的传统类型犯罪带来的刑事风险。目前,网络空间已经成为人类生活的第二空间,与传统物理空间不同,网络空间具有开放性、共享性和隐蔽性,网络犯罪借助网络空间不断蔓延滋生,已经成为当前的主要犯罪类型之一。一旦发生网络攻击行为,网络的稳定运行状态将被破坏,网络数据的保密性和可用性也难以得到保证;传统类型的犯罪行为在发生的物理空间上具有局限性,而网络空间的开放性导致该领域犯罪相较于传统类型的犯罪来说,受害人的分布区域更广泛,以及因其隐蔽性特点带来的刑事侦查难度大的问题。为避免出现上述情况,网络服务提供者在主要地承担网络空间的构建以及网络规则的制订的过程中,需要更加切实地履行网络空间安全管理义务。《中华人民共和国网络安全法》(简称《网络安全法》)第 9 条明确针对网络运营者规定了包括"履行网络安全保护义务"在内的六项基本任务,原则上确立了网络运营者系网络安全的第一责任人,其安全管理义务的主要内容是在数据全生命周期维护包括存储硬件设施安全、软件系统安全和数据安全在内的各项网络空间安全,并在未履行法定义务时承担相应的法律责任。如果网络技术或服务存在不当漏洞,就很可能被网络犯罪利用,使得网络技术或服务提供者涉嫌刑事犯罪。《中华人民共和国刑法修正案(九)》确立了拒不履行信息网络安全管理义务罪,《刑法》第 286 条之一规定该罪的犯罪主体

① 参见北京市第一中级人民法院(2021)京 01 刑终 542 号二审刑事判决书。

② 参见山东省临沂市中级人民法院(2018)鲁 13 刑终 549 号二审刑事判决书。对于该案中是否起诉单位犯罪,法检存在争议。

是网络服务提供者,刑事责任的前提要素为经监管部门责令采取改正措施而拒不改正,即网络服务提供者基于事实认识错误或法律认识错误而拒绝改正,将有可能触犯该罪。值得注意的是,《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》(简称《信息网络犯罪司法解释》)同时明确了因拒不履行网络安全管理义务,致使危害国家安全犯罪等特定犯罪案件证据灭失、多次造成刑事案件证据灭失等情形属于"情节严重"。以造成危害国家安全犯罪证据灭失为例,该情形不要求行为人具备危害国家安全的主观故意,若行为人具备危害国家安全的主观故意,则可能构成拒不履行信息网络安全管理义务罪和危害国家安全罪的法条竞合。

从犯罪构成来看,拒不履行信息网络安全管理义务罪的适用较为泛化,导致相关企业和个人触犯此罪的风险较高、安全管理义务较为严格。一是"技术中立"的抗辩不被认可,中立服务性质的行为,具有日常性、职业性等特点,故一般不作为犯罪处理,例如,仅为互联网提供接入服务的行为通常不认为是犯罪行为,但是拒不履行信息网络安全管理义务罪的入刑已经说明,中国现行刑事立法已经否认网络服务提供者中立帮助行为作为合理抗辩理由的资格。根据《刑法》第286条之一的规定,只要网络服务提供者经行政机关责令改正而拒不改正,且具有四种情形之一的,就应当受到刑事处罚。在这个问题上,"快播案"曾经引发广泛争议,但法院最终仍然判处快播公司的行为构成犯罪。① 二是此罪系不作为犯罪,以行为人具备信息网络安全管理义务为前提。但信息网络安全管理义务的范围并没有被法律明确规定,这就需要参照其他法律、行政法规的规定。② 目前,法律法规对网络服务提供者的信息网络安全管理义务作出的相应规定较为局限,主要可见于《网络安全法》以及《全国人民代表大会常务委员会关于加强网络信息保护的决定》的相关内容,义务范围涉及信息网络制度构建、用户安全教育、违法信息备案等网络数据全生命周期,这种泛化的义务规定导致相关主体违反义务的可能性大幅提升。三是后果严重的程度要件标准过低。根据《信息网络犯罪司法解释》,网络服务提供者拒不履行信息网络安全管理义务,经监管部门责令采取改正措施而拒不改正,致使泄露个人隐私信息500条以上的,就达到入罪标准,而网络空间中数据信息动辄数以万计,这意味着对于涉案企业而言,如果没有履行监管部门规定的信息网络安全管理义务,就存在"一泄露就入罪"的严重风险。③

就罪数问题而言,违反信息网络安全管理义务可能涉及的刑事风险包括:一是涉及单一犯罪,如拒不履行信息网络安全管理义务罪的单一犯罪;二是存在犯罪竞合,如实施涉及数据的侵犯公民个人信息罪或者通过网络暴力等行为实施了寻衅滋事罪,同时构成拒不履行信息网络安全管理义务罪的,依法应当择重处罚,换言之,即构成本罪的同时又是诸多网络犯罪的共犯,但共犯原理如何对其进行解释,仍然存在进一步完善的空间。例如,在"快播案"中,快播公司对其提供的视频含有色情内容是充分明知的,经行政机关处罚仍然不履行监管职责,放任公司控制和管理的缓存服务器上存储并进一步传播相关淫秽视频,构成拒不履行信息网络安全管理义务罪。拒不履行信息网络安全管理义务入刑意味着网络服务提供者面临的刑事风险大幅增加,如果未能积极履行信息网络安全管理义务,企业将面临巨额罚款、甚至破产倒闭的严重后果。

(三)数字知识产权刑事合规风险——法益维度

上文已提到客体及空间两个维度,还可以从法益维度思考数字知识产权刑事合规风险问题。在对案件进行类型化分析的背景下,可以看到侵害的法益类型是多种多样的,而其中占比较大的法益类型为数字知识产权类型。针对该问题,应当作出两个前置性的说明:首先,虽然在中国犯罪论构成体系尚未固定的情况下,犯罪客体和法益往往处于混同的状况,但是笔者仍然希望作出区分,尤其是将客体作为法益的一种承载者,从而保证客体具有一定的可查性、客观性和具体性。盖因,宪法是确定刑法保护对象的根据,以法益来作为刑法保护对象更有利于规范、明确地表达犯罪所侵犯的公民基本权利或宪法所维护的制度、价值,更有利于实现宪法与刑法的沟通互动。简言之,法益更为接近法律价值层次。其次,刑法的目的在于保护法益已经逐渐成为共识,而某项利益,尤其是目前遭受极大风险威胁的利益,只有经过一定的审查之后才能被界定为法益,可见,法益本身作为一项法律构建,因其定型性和沟通性的特质,可以实现刑法与社会之间的良性互动。

① 争论观点可参见《车浩新评快播案:法律无需掌声,也不能嘲弄》,载微信公众号"中国法律评论"2016年1月22日,https://mp.weixin.qq.com/s/cIS8CJZ1--7g4dTDTpXewQ。

② 参见敬力嘉:《信息网络安全管理义务的刑法教义学展开》,载《东方法学》2017年第5期,第82页。

③ 参见周维明:《刑事合规视野下数据犯罪的治理路径》,载《西南政法大学学报》2022年第5期,第130页。

理论上,法益论可以容纳更多具体内容,诸如刑事政策等社会政策、民众意见,从而成为刑法内外的共同指涉,具有一定的类型化功能。

数字经济发展离不开知识产权,在数字经济时代下,知识产权犯罪更易发生、更难发现、影响更广。上海市杨浦区人民法院、上海市杨浦区人民检察院联合发布的《涉数字经济犯罪案件司法白皮书(2018—2022年)》显示,①在 282 起知识产权犯罪案件中,大多数案件涉及销售假冒注册商标的商品,共 180 起,占63.83%;侵犯著作权罪案件 15 起,占 5.32%,涉及未授权销售或以技术手段批量复制作品。北京市检察院知识产权办公室在对 2020 年至 2023 年 6 月全市检察机关办理的侵犯知识产权犯罪刑事案件进行梳理时发现,北京市检察机关在前述期间共办理侵犯数字经济领域知识产权刑事案件 37 件,约占侵犯知识产权犯罪刑事案件总数的 40%。其中,案件集中在侵犯著作权罪、侵犯商业秘密罪等罪名。② 数字经济领域知识产权刑事案件呈现四大特点,具体展开如下。

一是侵犯知识产权犯罪与网络犯罪紧密结合。数字经济领域的知识产权犯罪,体现为侵犯知识产权犯罪与网络犯罪的相互交织,主要为利用爬虫、“撞库”和云存储等技术手段进行网络犯罪,犯罪分工细致,对个人信息和数据安全构成严重威胁。

二是数字服务软件成为新的侵权对象。数字经济的快速发展以大量数字服务软件的生产和使用为依托,这些软件如数据模型和云服务平台软件等成为热门的侵权对象。

三是侵犯商业秘密案件的犯罪主体多为企业内部员工。数字企业的专利技术和产品参数等信息是企业维护自身数据安全性的重点,尽管采取了许多加密措施,但仍然会产生重要商业秘密被非法窃取的情况。这类案件的行为人大多数为企业内部员工,其在职期间以正当方式获取商业秘密但非法传递给他人,或者非法占有关键信息并在离职时窃取信息用于非法牟利。

四是被侵权企业的证据留存能力不足。部分案例显示,企业因被侵权后缺乏保留证据的能力,导致了遭受犯罪侵害之后维权困难的情况。侵犯商业秘密案件的一个关键性问题是判断“秘点”,若被侵权的企业无法提供有效证据,可能造成因证据不足而使犯罪嫌疑人脱罪的负面结果,这本可以通过建立企业数据保存和传输的保密安全系统制度而得以避免。

之所以将数字经济本身作为一种独立的法益类型,系其本身具有复合性。一种是横向之复合性,即传统意义上不同类型的法益同时容纳在数字经济场景之中;另一种是纵向之复合性,即如果不保全数字经济秩序法益,那么将会侵犯知识产权、个人数据、隐私信息等法益类型,同时也会因为在程序法上面临困难,引发由一个危险造成的更为广泛的危险。

(四)其他主要的刑事合规风险

除了上述三种相对“总论性”“总则性”的类型化方案之外,还有部分属于所谓的“修正构成要件”的内容。刑法理论上中国学者往往认为某些犯罪虽然是针对新兴法益,但可以通过共同犯罪原理等解释出来,因此没有规定的必要性;但是实践中往往会将此类犯罪作为独立的类型。最典型的就是帮信罪,其本身是信息网络活动犯罪的帮助犯,但基于某些理由而成为单独的罪名。刑法理论很难给出一个统一的答案,从而回应“正犯化”的做法。目前虽然存在一些有力学说,例如复合法益说等,承认这些罪名具有的独立目的,然而,笔者认为这些理论尚存没有处理的问题,例如,无法解决洗钱罪与帮信罪之间存在的核心区别。有鉴于此,在上述“总论性”的类型化方案之外,笔者还关注到部分对数字经济影响巨大,但并非处于中间地位,无法作为实行行为之正犯的类型,具体详述如下。

1.广告合规(虚假行为)

受新冠疫情影响,直播带货行业迅速崛起,众多购物直播平台相继出现,这不仅带来了一种极具规模和影响力的商业模式,也很大程度地改变了人们的消费习惯。根据网经社电子商务研究中心联合中国商业联合会直播电商工作委员会发布的《2023 年(上)中国直播电商市场数据报告》,2023 年上半年,中国的直播电

① 参见上海市杨浦区人民法院、上海市杨浦区人民检察院:《涉数字经济犯罪案件司法白皮书(2018—2022 年)》,载上海市高级人民法院网站 2023 年 7 月 10 日,https://www.hshfy.sh.cn/css/2023/07/10/20230710143811285107 5.pdf。

② 参见简洁、王晨:《数字经济领域知识产权刑事案件呈现四大特点》,载《检察日报》2023 年 8 月 29 日,第 7 版。

商交易规模约为19 916亿元,预计全年将达到45 657亿元,同比增长30.44%。[①] 由此可见,直播电商已经成为一股重要的新兴经济势力,对该领域的刑事合规风险予以重点关注十分必要。

在直播电商领域较为常见的犯罪类型是虚假行为,其主要表现形式包括虚假广告、流量造假和销售假货等,反映出了虚假行为的共性。小红书或抖音等平台都曾出现许多虚假广告,例如宣传保健品的神奇功效或夸大美容手术服务的效果等。这些广告不仅存在侵犯消费者身体健康的风险,同时严重扰乱了市场经济秩序。电商主播或者社交媒体博主与品牌方签订服务协议,作为广告发布者为其在平台通过直播销售或分享使用体验的积极评价等方式对产品进行宣传,如所发布广告存在虚假成分,则构成《刑法》第222条所规定的虚假广告罪。具体实践中,由于主播们利润最大化的逐利心态,虚假广告犯罪大量存在于各大平台,使得该类犯罪行为呈现出范围广、影响大的特征。

另一种虚假行为体现为流量造假,具体是指商家利用技术手段虚构并夸大实际客户流量从而达到获取非法利益的行为。数字经济以流量作为重要的经营指标,主播们倾向于通过虚构流量从而夸大自身品牌的市场受欢迎程度,以不正当手段获取更多客源。在技术层面,流量造假的实现方式主要包括Cookie不断跑量、IP地址更迭及分散所在地以及非法获取并分析Click来源。[②] 大部分主播为个体户经营模式,也存在相当数量的头部主播隶属于大型经纪公司。根据《刑法》第231条的规定,经纪公司通过流量造假行为获取非法利润,需承担单位刑事责任;如果单位旗下的主播构成虚假广告罪,那么单位的主管人员及相关责任人同样按虚假广告罪进行定罪处罚。[③]

除了虚假宣传外,由于平台往往缺乏严格的监管规则,产品质量问题也在网络直播带货领域频频出现,不仅对平台和主播的声誉产生极大的负面影响,而且严重损害了消费者的利益。《刑法》第140条规定的生产、销售伪劣产品罪规定了销售者可作为该罪的犯罪主体,并且在满足掺杂、掺假,以假充真,以次充好或者以不合格产品冒充合格产品,以及销售金额超过5万元的客观要件前提下,可能构成本罪。根据《刑法》第214条的规定,依托电商直播平台销售"山寨产品"涉嫌构成销售假冒注册商标的商品罪。这种类型的销售模式比传统的线上或线下销售模式的传播速度更快,观看直播的观众缺乏实地验货的可能,仅凭对主播的喜爱就下单购买,直播的产品链接缺乏必要的核验信息,加剧了消费者的购物风险。主播号召力越大,其造成的受害者人数也就越多,损害金额也就越大。若违法所得数额巨大或者有其他严重情节的,处三年以上七年以下有期徒刑并处罚金。根据《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释》第2条,"数额巨大"即销售金额超过二十五万元,头部主播的销售活动很容易达到该数额以致面临严重刑责的风险。

2.经营合规(垄断行为)

目前头部主播往往通过"全网最低价"的噱头来吸引消费者,不但造成主播和品牌方的利益纠纷,同时也涉嫌滥用市场支配地位,造成其他小主播以及实体店铺经营者的客源大量流失,干扰了正常的市场经济秩序。在"京东平台自费补贴事件"中,海氏某款烤箱在京东平台上的价格低于品牌方与主播李佳琦签约的直播售价,造成品牌方海氏被动违反了与李佳琦签订的"底价协议"从而将面临巨额违约金。[④] "底价协议"看上去使得消费者获得了优惠价格的产品,但在优惠的背后是头部主播的"底价协议"本身所带来的垄断行为的嫌疑。对于"底价协议"是否构成垄断,首先需考察其是否违反《中华人民共和国反垄断法》(简称《反垄断法》)和其他反垄断相关法律法规,以及是否满足垄断行为的相关构成要件;其次需考察"底价协议"是否产生排除或者限制竞争的后果,是否通过价格控制侵害了消费者的合法权益和市场公平竞争。[⑤]

2021年《国务院反垄断委员会关于平台经济领域的反垄断指南》第7条第2款提及平台经营者要求平台内经营者向其提供等于或优于其他竞争性平台的交易条件可能构成垄断。《反垄断法》虽然将大部分垄

① 参见张一鸣:《2023年上半年直播电商交易规模稳步增长》,载《中国经济时报》2023年8月28日,第4版。

② 参见李谦:《流量造假的刑法治理》,载中华人民共和国最高人民检察院网站2020年12月21日,https://www.spp.gov.cn/spp/llyj/202012/t20201221_489489.shtml。

③ 参见上海中申律师事务所知产/商事部:《直播带假货,主播要承担哪些法律责任?》,载上海中申律师事务所网站2021年1月2日,http://law-zs.com/news/44.html。

④ 所谓"底价协议",是指主播与品牌方达成的某种价格协议,约定在某一时间段内其他任何销售渠道的售价都不得低于其直播间价格。

⑤ 参见顾平安、张强:《直播带货的底价协议是否构成垄断》,载《学习时报》2023年11年24日,第A3版。

断行为(如滥用市场支配地位)的处罚仍限制在行政处罚的规范框架之内,但也确认了垄断行为的可罪责化。[①] 根据法律规定,带货主播并未被排除于犯罪主体的范围之外。目前中国刑法中尚未有关于垄断行为罪责的条款,后续是否通过刑法修正案予以修改值得关注。将垄断行为罪责化面临的问题主要在于:入刑边界不明确导致难以激活刑事责任条款;对于是否构成反垄断行为的判断之专业性与复杂性也将增加刑事责任条款适用的难度。

三、数字经济刑事合规风险的规制路径

分析数字经济刑事合规风险的多维面向之后,需结合目前的企业刑事合规实际,提出切实可行的规制路径。从方法论角度,需首先明确规制的基本原则,理清基本逻辑,继而提出具体的实践路径。

(一)数字经济刑事合规风险规制的基本原则

1.激励原则

激励是一种心理学概念,在学术领域中通常被描述为能够引发特定主体采取某种行动的内在或外在的驱动力。这种驱动力不仅对于个体的行为动机具有关键作用,而且在组织或群体层面上,能够显著地提升目标导向行为的积极性,从而有助于实现集体或组织的目标。激励理论是研究领域中专注于探讨如何增强人的积极性的一系列学说和理论。这些理论从包括心理学、经济学、社会学在内的多个角度深入研究了人类行为背后的动机,以及如何通过这些动机来影响和改变人们的行为。

在数字时代,随着数据成为企业和社会的重要资源,数字刑事合规的重要性也逐渐凸显。数字刑事合规不仅是一套为了确保员工严格遵守与数字资源使用相关的法规和标准而设计的管理策略,还是政府部门为了监督和推动企业依法、合规利用数字资源而采用的一种重要的外部激励机制。这种机制通过一系列的政策、法规和监管措施,确保企业在使用数字资源时不仅符合法律的规定,还能在道德和社会责任方面达到更高的标准。20 世纪末以来,企业合规机制得到了广泛的实施和应用。作为一种重要的管理工具,合规计划在其中发挥了核心作用,其不仅为企业提供了一套明确的行为准则和操作规程,还在某些情况下,为违法企业提供了刑事和行政上宽大处理的可能性。宽大处理通常作为一种激励机制,鼓励企业自主建立并有效实施合规计划,从而在法治的轨道上更加规范、透明地开展业务活动。通过这种方式,企业不仅能够降低自身的法律风险,还能在社会上建立良好的声誉和信誉,从而为其长期的可持续发展奠定坚实的基础。

在中国企业积极推进数字合规建设的进程中,激励理论的指导作用显得尤为重要,企业应构建一套全面而有效的激励机制,以推动数字合规的深入实施。具体而言,这一激励机制应包含三个维度。

一是构建行政宽大处理的激励机制。在这一机制下,数字合规被视为行政和解的适用条件以及减轻行政处罚的重要依据。这意味着,对于在数字合规方面表现良好的企业,行政部门在处理相关违规行为时可以采取更为宽大和灵活的态度,通过行政和解等方式减轻或免除处罚,从而鼓励企业更加重视数字合规建设,形成积极的合规文化。

二是建立刑事宽大处理机制。在这一机制下,数字合规被作为不起诉的依据、无罪抗辩或减免刑罚的理由。同时,其也可以作为签署暂缓起诉协议和撤销起诉的依据。这一机制的实施,不仅有助于鼓励企业在面临刑事风险时积极配合调查和整改,更重要的是,通过将数字合规与刑事责任相挂钩,提升了企业在数字合规方面的自觉性和主动性。

三是确立国际组织的制裁消除机制。随着全球经济一体化的深入发展,中国企业越来越多地参与到国际经济活动中。在这一背景下,企业数字合规不仅关系到国内法规,还与国际组织的制裁措施密切相关。因此,将企业数字合规视为附条件或无条件减免国际组织制裁的依据,对于激励企业在国际舞台上展现良好的合规形象具有重要意义。

还需要注意,上述激励措施并不一定是程序性的,刑事实体法也可以出于法益等的综合考量,适度将刑事合规的部分思想吸纳到犯罪认定的路径之中,构建恰当的出罪机制。

---

① 《反垄断法》第 67 条规定:“违反本法规定,构成犯罪的,依法追究刑事责任。”

2.权利义务相一致原则

权利与义务相一致原则是企业数字刑事合规应当坚持的原则,权利指向的是公民的数字权利,义务指向的是企业的数字义务。首先,法律应当确保公民的基本数字权利得到充分的保障。《中华人民共和国个人信息保护法》第1条开宗明义地指出,其立法目的系“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”,《中华人民共和国民法典》第111条规定自然人的个人信息受法律保护,第1038条要求信息处理者采取技术措施和其他必要措施,确保其收集、存储的个人信息安全,防止信息泄露、篡改、丢失。从前述规定中可以看出,数字时代背景下的个人信息数据权利为当下法律体系所重点保护的对象。更为重要的是,数据保护相关法律的严厉性体现了立法者的态度,即不仅仅是对个人信息安全的一种简单维护,更深层次上体现了对公民尊严和自由的尊重与保护。这种保护机制可以被视为对宪法所赋予的公民基本权利的一种具体保障,其最终的目的在于维护人的尊严不受侵犯。因此,保护个人数字信息在现代法律体系中占据了举足轻重的地位,其不仅是法律对公民基本权利的一种外在保障,更是人格权保护不可或缺的重要组成部分。

与公民的数字权利相对应,企业肩负着全面履行数字义务的重任。这种权利与义务之间的对应关系是现代企业伦理和社会责任理论的基石。企业的数字义务不仅涉及数据的收集、储存和使用,更关系如何确保这些数据的安全性和合规性,以及如何在利用这些数据推动业务发展的同时尊重和保护相关方的数字权利。在这个框架下,企业数字义务的履行可以被视为公民数字权利得以实现的前提条件。为了确保公民的数字权利(如隐私权、信息安全等)不受企业活动的侵害,企业应始终将履行数字义务作为经营活动的核心指导原则。这意味着,企业在日常运营和决策过程中,对数字义务的遵守和履行应优先于其他商业考虑。这种对数字义务的坚守不仅有助于企业建立良好的社会声誉和信誉,更是对公民数字权利最直接和最有效的保障。通过这种方式,企业不仅在法律层面履行了其应尽的责任,更在道德和社会责任层面展现了其对社会和公众的承诺。

3.系统性治理原则——以企业内部合规管理体系为重点

刑事合规需要各级行政机关和司法机关的协调配合,同时需重点关注企业层面的合规理念引导以及相应的合规制度设计。从刑事合规理念层面来说,企业核心层(最高管理者)的高度重视具有重要作用,确保构建一套高效的内部合规管理体系,对于促进刑事合规管理的成功具有决定性意义。为达成上述目标,企业应立足于自身内部管理架构的实际情况,精心打造一个由管理层发挥领导作用、全体员工积极参与的数字合规管理体系。具体来说,企业应成立专门的合规管理机构,该机构具备独立性,其职能与职责需得到明确,确保其资源配置与企业整体战略和业务需求相匹配。从目前国内企业的法务部门所承担的职责角度来说,应多落脚在企业劳动合规、商业合作各类协议等书面合同的撰写及企业与外部单位产生的法律争端的解决等方面。大部分企业其实并未建立完善的法律风险控制体系,遑论数字经济刑事合规风险控制体系。换句话说,企业合规从以自律为中心的粗犷合规阶段(第一阶段),过渡到从20世纪60年代发展起来的基于现代理念的企业合规阶段(第二阶段),接着步入企业刑事合规阶段(第三阶段)。第二阶段与第三阶段有所不同,具体而言:第二阶段主要以民法和行政法规制为主,而第三阶段以刑法规制为主,这又极大地仰仗相应的法律研究(经济刑法和单位犯罪的研究)以及相应配套的企业合规激励制度和与上述相适应的法律制度。[①]要做好数字经济的刑事合规,企业自身提高合规意识毫无疑问是非常重要的,不仅需要企业发挥主观能动性,也需要司法部门进行更多的企业刑事合规普法宣传作为犯罪预防,并通过对企业(作为受害者或者加害者)的数字经济刑事犯罪依法进行刑事处罚或行政处罚进行多方位配合。

企业刑事合规的最主要角色就是企业本身,最重要的措施就是及时建立企业内部的合规管理机构,并且在行政层级上保持相对的独立性,从而更有效地履行其监管和指导职责。该管理机构需注重事前预防和事后预防:在事前预防部分,应提前分析企业运营阶段可能产生的各类刑事合规风险,并针对各种风险制定相应的合规制度;同时,企业合规部门也需要做好事后预防,即针对预期即将面临的合规风险以及已经实现的合规风险。以德国为例,从2024年年初开始,德国政府要求人数达到一定规模的企业需设置内部举报机构,

① 参见赵赤:《刑事合规是企业合规发展迭代新样态》,载《检察日报》2023年1月19日,第3版。

该机构可以设置在企业内部,也可以任务外包(让外部公司承担接收举报信息的职能),该设置为企业的强制性义务。企业内部举报机构独立于其他任何部门并直接对企业主体负责,为企业合规方面的一项重要举措。德国的企业内部举报制度主要体现的就是一种事后预防。① 同时,需注重企业部门与部门之间的协调:合规管理机构与企业内部其他部门建立协同合作关系,这是实现全面有效的合规管理的重要环节。通过强化部门间的沟通、协作与信息共享,形成一个相互支持、相互制约的良性互动机制,进一步提升企业内部合规管理的整体效能。

系统性治理是一种全面且综合的治理范式,其核心在于以公众需求为导向,并深度利用信息技术作为实现手段。这种治理方式强调协调、整合与义务等机制的运用,以有效跨越传统组织间的功能界限,从而实现对多层面、多维度问题的协同治理。政策颁布和法律制定之间存在时间跨度,公私部门协同工作效果不佳,数据犯罪调查取证困难,都显示了数字经济刑事合规的困难。这些问题往往导致治理效率低下、资源浪费和公众满意度降低。通过系统性的协调与整合,这种治理方式旨在打破原有分散、部分和破碎的治理格局,逐步构建起集中、整体和整合的治理结构。

在数字合规的风险防范过程中,系统性治理还强调利用信息技术的优势,推动治理由分散向集中、由部分向整体、由破碎向整合的转变。这种转变不仅有助于提升治理效率,更能为公众提供更加全面、高效的整体性服务,从而增强公众的获得感和满意度。从更深层次来看,系统性治理体现了国家治理的包容性和整合性。包容性体现在对多元利益诉求的尊重和平衡,整合性则体现在对碎片化问题的综合协调和整合。这种治理方式不仅是现代社会治理的重要发展方向,更是国家治理体系和治理能力现代化的关键路径之一。

具体而言,系统性治理理论对数字合规治理的重要意义体现在多个层面。首先,这一理论坚持以公众需求为导向的治理原则,将民众对数字安全的迫切期望置于治理的核心位置。这种以人民为中心的理念,确保了治理措施与公众需求的紧密契合,从而增强了治理的针对性和实效性。其次,系统性治理理论强调通过协调、整合和义务等机制,跨越部门管理边界进行合作的重要性。这种合作方式从传统行政主管部门单打独斗转变为行政、司法等多元力量的协同配合,实现数字合规的全方位保障。② 这种跨部门、跨领域的合作形成的强大治理合力,有助于治理效能的提升。再次,在治理手段方面,系统性治理理论倡导充分利用数字技术和传统治理手段互相进行有机整合,更好地实现了治理手段的优化配置。这种综合性的治理手段能够应对数字时代复杂多变的挑战,为公众提供全面、高效的整体性服务。通过数字技术的广泛应用和不断创新,结合政策引导、法律规范、服务提供和监督保障等手段的综合运用,可以构建起一个立体化的数字合规治理网络,确保数据安全和隐私保护的有效保障。最后,系统性治理理论强调政府和企业在数字合规治理中的积极参与和协同作用。虽然政府部门的监管在数字合规治理中发挥着重要作用,但是外因的作用无法与内因的作用相提并论(内因即企业的自觉性和主动性)。推动企业对数字合规采取更为重视的态度,发挥其内在积极性并由被动转为主动,是实现可持续性发展的关键所在。政府和企业应共同努力,形成紧密的合作关系,共同推动数字合规治理的深入开展。

(二)数字经济刑事合规风险规制的基本逻辑

1.刑事合规数字平台建设

在基础逻辑层面,为实现数字合规风险防控,企业应依据数字合规准则,系统性地加强其平台构建。此过程涉及对企业数字合规环境的全面认知,以及对关键风险因素的精确识别。

宏观层面上,企业应深入探究其所在国家或地区关于数字管理的法律条文及政策导向,理解并预测其未来发展趋势。对宏观法律环境的全面认知有助于企业在制定数字合规策略时,确保与法律法规的一致性,从而避免潜在的法律风险。

中观层面上,企业应当对其所在行业的数字合规标准进行细致剖析,这涉及对行业内的最佳实践、行业标准以及竞争对手的数字合规策略的深入了解。通过这种分析方式,企业可以在行业背景下定位自身的数

① European Parliament and Council of the European Union, *Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the Protection of Persons Who Report Breaches of Union Law*, Official Journal of the European Union (26 November 2019), https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=CELEX:32019L1937.

② 参见贾宇:《数字经济刑事法治保障研究》,载《社会科学文摘》2023 年第 6 期,第 17 页。

字合规水平,发现并弥补与行业标准的差距。

微观层面上,企业应全面审视自身的数据利用倾向、业务模式和战略规划,确保上述元素与数字合规要求相协调。这意味着企业需要在日常运营中融入数字合规理念,在数据的收集、处理、存储到使用的全生命周期,都应遵循数字合规的基本原则。

此外,需要明确加强数字合规风险管控的核心业务或岗位范畴。这要求企业对内部运营进行全面梳理,识别出潜在的风险点,并对这些关键点实施针对性的风险管理措施。同时,企业应建立有效的风险评估和监控机制,实时跟踪数字合规风险管控的发展动向,确保在风险事件发生时能够迅速应对。

2.刑事合规风险监测与预警机制

考虑到数字经济时代企业的经营活动日益依赖于数据和网络,企业面临的合规风险呈现出新的特点和趋势。对此,在基本逻辑层面上,应当要求企业建立刑事合规风险监测与预警机制,具体而言可以分为刑事合规风险监测机制和预警机制。

首先,刑事合规风险监测机制是企业及时识别和评估合规风险的关键。在数字经济环境下,企业应当构建一套完善的合规风险监测体系,通过定期的数据收集、分析和报告,全面把握企业在数据处理、网络安全、知识产权保护等方面的合规状况。同时,监测机制还应关注行业动态和法律法规的变化,确保企业的合规策略始终与外部环境相适应。

其次,预警机制能够在风险事件发生前提供早期信号,为企业采取预防性措施赢得宝贵时间。通过建立一套科学的预警指标体系,结合先进的数据分析技术,预警机制可以对潜在的刑事合规风险进行实时跟踪和预测。一旦检测到异常情况或风险上升趋势,预警机制应立即启动应急响应程序,通知相关部门采取必要的风险管控措施。

最后,刑事合规风险监测与预警机制的建立还需要企业在制度、技术和人员等方面进行全面投入。企业应当制定详细的合规风险管理政策,明确各部门在风险监测和预警中的职责与权限;加强信息系统建设,提高数据处理和分析能力;培养一支具备专业知识和技能的合规管理团队,确保刑事合规风险监测与预警工作的有效开展。

3.刑事合规风险监督与评估机制

除了刑事合规风险监测与预警机制之外,企业还应当建立刑事合规风险的监督与评估机制,建立风险监督与评估机制的基本逻辑如下。

首先,刑事合规风险监督机制应当独立于企业的日常运营,具备独立性和权威性,以确保监督工作的客观性和公正性。监督机制的主要职责包括对企业合规管理制度的执行情况进行定期或不定期的检查,发现并纠正合规管理中的漏洞和不足;对涉及刑事合规风险的关键业务和岗位进行重点监督,确保严格遵守法律法规和企业内部规定。

其次,刑事合规风险评估机制旨在通过对潜在风险进行定量和定性分析,为企业提供决策依据。评估机制应采用科学的风险评估方法和技术,结合企业内部数据和外部信息,对刑事合规风险进行全面、准确的评估。评估结果有助于揭示企业当前面临的刑事合规风险水平,也可以预测未来可能出现的风险趋势,为企业制定针对性的风险管理策略提供有力支持。

最后,刑事合规风险监督与评估机制的建立还需要企业在组织架构、制度建设和人员配置等方面进行合理安排。企业应设立专门的合规监督部门或岗位,负责监督机制的日常运作;制定完善的监督与评估制度,明确监督与评估的范围、程序和标准;加强人员培训,确保相关人员具备履行监督与评估职责所需的专业知识和技能。

(三)数字经济刑事合规风险规制的实践路径

1.针对数据安全(客体维度)

一是构建并持续优化数据分类分级保护机制。这一机制为企业数据的安全性与合规性提供了保障,并且有助于实现企业可持续发展的长远战略。为保障《中华人民共和国数据安全法》第21条“数据分类分级保护”的需求,各地区、各部门需据此调整内部规章制度,详细制定并不断完善适用于其管辖范围及所属行

业、领域的重要数据目录。[①] 这一举措旨在确保对于数据的精细化管理和有效保护,以应对日益复杂多变的数据安全风险。应根据数据收集和使用的不同阶段以及数据的类型,来制定相应的保护机制。在此背景下,数据密集型企业必须严格遵守法律法规的各项要求,积极履行企业的社会责任,精确识别并分类企业所持有的各类数据。针对不同类型、不同级别的数据,企业应制定相应的精细化合规管理策略,以确保数据的合规使用、安全存储和有效流通。可参考的标准有《基础电信企业重要数据识别指南》(YD/T 3867—2021),《金融数据安全 数据安全分级指南》(JR/T 0197—2020),此外,国家标准《信息安全技术 网络数据分类分级要求》(GB/T 43697—2024)已发布。

二是确立企业数据合规的核心层负责制以及完善相应数据合规制度。首先,应明确企业的核心层(最高管理者)是数据合规的第一责任人,并应当承担以下职责:企业内部资源优化配置以建立和完善数据合规管理体系;建立针对数据违规的内部举报机制;确保企业运营目标与履行数据合规义务之间的一致性;建立问责机制,明确企业内部数据违规行为的纪律处分和后果。[②] 具体展开来说,企业的法务部门通常并不具备数据法的专门知识,因此难以独立地作为数据合规管理部门以提供支持。企业数据方面的实际操作人员其实是企业运营过程中具体到网站和 APP 的数据收集和使用的运营部门,在具体网站和 APP 建设方面多采取外包服务,即大部分企业通常并不直接参与具体的网页和 APP 设计,而是作为甲方提出需求,所提出的需求和企业的基本业务流程的逻辑保持一致。较为合理的合规管理机构设置应是设立一个专门的数据合规部门,且该部门需协同法务部门和涉及企业数据部分的运营部门。由运营部门整理并提交数据使用和收集的正当、合理依据与方法,交由数据合规管理部门进行审查,数据合规管理部门可采取“公司法务部门+外部数据法专业律师”或者“公司法务部门+公司内部数据合规律师”的方式建立组织架构,并及时建立相应的企业数据安全规章制度。企业应及时设置内部举报机制,并且保证针对数据违规行为的举报过程是顺畅无阻的。企业也必须对数据合规建立正确的认识,正视合规的激励作用,同时做到权利义务相一致。企业也需保证在具体的数据违规行为发生后,可根据内部规章制度进行处分,如果行为严重至违法犯罪的程度,那么企业需及时向有关部门进行报告并提供相应的材料以配合调查。

通过上述的一系列综合措施,企业不仅能够提升自身的数据管理能力,降低数据泄露和滥用等风险,还能够为行业的健康发展和国家的数字经济建设作出积极贡献。

2.针对网络空间(空间维度)

《信息网络犯罪司法解释》的出台,体现了国家层面重视网络安全保护的重要司法导向。结合实务数据来看,构成拒不履行信息网络安全管理义务罪的数量标准并不高:如传播违法视频文件 200 个以上、泄露个人征信信息 500 条以上或者未留存网络用户日志。但以公司为主体进行犯罪,主管人员将面临受到刑事处罚的风险,这也给企业带来较高的法律风险,并且造成较大的经济损失。为实现数字经济刑事合规的深入建设,应当定期对企业的网络安全合规状况进行深入评估,这有助于企业不断识别并应对各种潜在的安全违规风险,进而维护企业声誉和保障业务连续性。为实现这一目标,应当加强以下方面。

一是明确企业的网络安全管理义务。根据《网络安全法》,网络运营主体分为一般网络运营者和关键信息基础设施运营者。针对上述不同的主体,需明确不同的网络安全管理义务,这也需要每个企业清晰认知自身定位,在此基础上建立相应的配套制度。

二是针对网络安全合规管理制度和实施机制的定期审查和评估。这一审查过程应全面而细致,旨在确保企业的网络安全管理制度能够与时俱进,与当前的法律法规和政策要求保持高度一致。通过这类审查,企业能够及时发现并修正制度中的不足或缺陷,从而确保网络安全管理制度的有效性和适用性;同时,针对网络安全合规实施机制进行定期评估。这一评估过程应注重实效,通过全面分析合规管理、审计、监察等部门间的协作程度,以揭示可能存在的协调不足或沟通障碍。这样的评估有助于企业持续优化内部流程,加强部门间的协同合作,进而实现网络合规管理体系与企业管理体系之间的协同性。这种协同性不仅可以提升企业的整体运营效率,还能够强化企业的风险应对能力。

---

① 参见张勇、李芬静:《数据安全刑事治理的冗余机制》,载《苏州大学学报(哲学社会科学版)》2023 年第 4 期,第 75 页。

② 参见上海市杨浦区人民法院、上海市杨浦区人民检察院:《企业数据合规指引 个人信息保护指引》,载上海市高级人民法院网站 2023 年 7 月 10 日,https://www.hshfy.sh.cn/css/2023/07/10/20230710144006555 4805.pdf。

三是针对网络合规管理人员工作绩效的定期评估。这也是提升企业网络安全水平的关键环节。通过对管理人员业务能力的持续评估,可以确保他们具备足够的专业知识和实践经验来有效应对网络安全挑战。评估应结合定量和定性指标,既考察管理人员的日常工作表现,也要关注他们在应对突发事件或复杂问题时的决策能力和应变能力。通过综合评估,企业可以及时发现管理人员的不足之处,并提供必要的培训和支持,以促进他们的专业成长和持续发展。

3.针对数字知识产权(法益维度)

在数字知识产权合规层面,应当完善数字知识产权的管理机制。具体可以从以下几个方面入手。

首先,应当建立一个全面的数字知识产权合规框架,该框架应包括合规政策、流程、培训、监控、风险评估和应对机制等多个方面,基于国内外相关法律法规、行业标准以及企业实际情况,确保企业在数字知识产权方面的行为符合法律要求和道德规范。同时,还可以通过定期的法律培训和合规宣传,提高全体员工对数字知识产权的重视程度和法律意识,鼓励员工自觉遵守相关规定,主动防范和抵制侵权行为。

其次,在流程层面上,企业应建立健全数字知识产权申请、保护和管理流程,确保数字知识产权的及时申请、有效保护和合规管理,以此加强对数字知识产权的维权力度,积极应对侵权行为,维护企业的合法权益。企业可以定期对自身的数字知识产权进行风险评估,识别潜在的风险点和侵权行为,建立相关的预警机制,对可能引发侵权纠纷的行为进行及时预警和干预,降低侵权风险。

最后,随着科技的发展,大数据、人工智能等先进技术为数字知识产权合规管理提供了新的解决方案。企业应积极利用这些技术手段,对海量的数字信息进行高效、准确的处理和分析,提高合规管理的效率和准确性。例如,可以利用大数据技术对侵权行为进行实时监测和追踪;利用人工智能技术对数字内容进行自动识别和分类,辅助判断是否存在知识产权侵权行为。

(四)其他配套管理机制建设

1.强化对于数字合规的外部监管

在数字经济快速发展的时代背景下,数字企业的合规经营问题日益凸显。为了确保数字企业在日常运营中严格遵守数字合规要求,外部行政监管的强化显得尤为关键。这种监管不仅是一项基础性的工作,更是实现数字企业合规发展的先决条件。从更深远的意义上说,“严格监管实则深层关怀”的理念在数字企业的监管工作中同样具有高度的适用性。①

当前,随着大数据技术的广泛应用,相关的行政监管部门在执行对数字企业活动的监管时,面临着更为复杂和多元的挑战。对大数据相关技术、设备和服务供应商的风险评估和安全管理工作应当得到加强,同时,大数据产业链上的各个环节应得到全面、深入的分析和评估,确保数字企业在使用大数据技术和服务时能够遵循相应的安全标准和合规要求。

此外,为了促进大数据产业健康、有序发展,应及时建立一套大数据标准体系。该体系涉及的方面包括大数据的基础、技术、应用和管理等。通过制定和实施统一的大数据标准,可以促进数字企业之间的数据互通和共享,提高数据的利用效率和价值,同时也有助于降低数字企业在数据处理和分析过程中的合规风险。与此同时,监管部门还应加速构建政府信息采集及使用的技术标准,同时涉及采集、存储、公开、共享、使用、质量保障和安全管理等方面。② 这些标准的建立和实施,有助于规范政府信息的使用和管理,确保政府数据在公开共享的同时,也能够得到有效的保护和管理。

最后,为了确保数字企业能够严格落实数字合规要求,监管部门应通过严谨的行政执法,依法追究违法者的法律责任。这要求监管部门建立健全的执法机制,加大对违法行为的查处力度,形成对数字企业的有效威慑和约束。同时,监管部门还应加强与司法机关的协作和配合,确保对违法行为的查处和追究工作能够依法进行并取得实效。

2.推进数字刑事合规立法

数字合规问题的根本解决之道在于明确的法律支撑。法律作为社会公正的维护者和行为规范的制定

① 参见齐鹏云:《企业数据合规官的治理边界及其规范体系》,载《信息资源管理学报》2023年第6期,第93页。

② 参见孙佑海:《我国企业数据合规的理论基础、现实检视与路径选择》,载《贵州大学学报(社会科学版)》2023年第6期,第84页。

者,对于数字合规问题的解决具有不可替代的作用。在当前中国法治建设的背景下,应当根据数字经济的刑事合规情况对刑法及刑事诉讼法等相关法律法规进行及时的修订。修订时应当充分考虑数字化时代的新特点和新挑战,确保法律条款能够与时俱进,为企业在数字化进程中的合规行为提供明确的法律依据。

在推进数字经济刑事合规立法的同时,需完善程序法和实体法,从而实现犯罪预防的企业化以及企业治理的法治化。针对企业犯罪的特殊性,有学者建议在未来立法中将附条件不起诉与认罪认罚从宽制度予以区分,并注意相应立法与其他合规的关联,具体需注意制度衔接、处罚衔接、规制衔接等方面内容。① 笔者建议,针对数字经济领域的犯罪复杂性以及隐蔽性特征,需考虑其多维度面向即客体维度、空间维度和法益维度的特征,具体问题具体分析,而不囿于对过往传统类型犯罪的固化理解。

3.促进数字合规的协同治理

在数字合规的建设过程中,数据流动是合规所关注的重点。由于数据本身具有高度的流动性特征,对于数据合规必然需要协同共治。在中国当前的数据应用生态中,数据的利用主要集中在组织内部的管理层面,而在跨部门、跨地域、跨行业的维度上,数据的开放、共享和协同应用尚处于初级阶段,存在诸多不足。这一现象限制了数据价值的最大化实现,也阻碍了数据作为重要生产要素在社会经济发展中的全面释放。为改变这一现状,需要从多个层面出发,加强数据的开放、共享和协同合作。要打破“数据孤岛”,推动数据在组织间、地域间和行业间的自由流动和高效利用。这要求政府、企业和公众共同努力,构建一个开放、包容、协同的数据生态环境。

一方面,在企业数据治理方面,应严格遵循“共建、共治、共享”原则。这意味着企业不仅要关注自身数据的收集、管理和利用,还要积极参与数据生态系统的共建,推动数据资源的共治和共享。通过构建一个开放性的生态系统,企业可以促进信息公开,提高公众参与度,从而增强数据的透明度和可信度。此外,为防止个别企业通过独占数据资源形成数据垄断,进而危害国家和人民的利益,需要建立有效的监管机制和法律法规。这些机制和法规应确保数据的公平竞争和合理利用,防止数据资源的过度集中和滥用。②

另一方面,需考虑公共数据的治理问题。各级政府机关和司法部门在行使各自职能的过程中收集了海量公共数据,其中也包括企业数据。对数据进行分级分类保护是责任更是义务。依法公开行政及司法程序中涉及的企业数据时,除了考虑社会监督的功能,也需注意公开内容以及公开方式,避免企业单位的数据权利在政府部门的信息公开过程中受到不当侵害。对于需要保密的国家秘密数据,政府部门应严格遵守《中华人民共和国保守国家秘密法》等相关法律法规的要求,采取必要的保密措施,旨在确保国家的数据安全和数据权益不受损害,维护国家的核心利益和人民的安全福祉。

四、结语

数字经济蓬勃兴旺,是数字时代发展到一定阶段的必然结果,随之而来的是巨额经济利润驱动下数据犯罪的乱象丛生。面对这样充满生机但又异常复杂的大时代,需要以一种严肃审慎的态度对这些新型数据犯罪进行调查和研究,并且深入考察与之相适应的刑事合规问题。数据权利作为一项重要权利需要受到法律多方面和多层次的保护,因此,应当建立并完善数据安全合规管理制度以及网络空间合规的监管制度,注意在具体追责方面的行刑衔接问题,进一步推动数据刑事合规方面的立法进程,及时回应数字时代对刑事法律的需要。

① 参见周振杰、李泽华:《以涉案企业合规改革推进刑事立法》,载《检察日报》2022 年 6 月 2 日,第 3 版。

② 参见孙佑海:《我国企业数据合规的理论基础、现实检视与路径选择》,载《贵州大学学报(社会科学版)》2023 年第 6 期,第 85 页。

Multi-Dimensional Analysis and Regulatory Path of Criminal Compliance Risks in the Digital Economy

Renagu APAER

(School of Law and Politics, Kashi University, Kashi 844000, China)

Abstract: In the context of the digital economy, while online platforms and data elements bring economic value to market entities such as enterprises, they also increase the potential for these entities to face criminal legal risks. Taking the behavior types of enterprises participating in the digital economy as the starting point, this article explores the criminal compliance risks that market entities may face in areas such as network data security, cyberspace security, digital intellectual property rights, as well as other key domains, and elaborates on these risks from the perspectives of object dimension, spatial dimension, and legal interest dimension. In the object dimension of criminal compliance risks related to data security, enterprises face risks of criminal compliance in data collection, data usage, and data management when organizing and applying data resources. In the spatial dimension of criminal compliance risks related to cyberspace security, besides considering the characteristics of criminal acts, criminal composition, and the issue of multiple offenses, attention should also be paid to other dimensions of crime in the digital economy, such as the spatiality of the internet. In the legal interest dimension of criminal compliance risks related to digital intellectual property rights, criminal cases related to intellectual property rights in the digital economy exhibit four main characteristics, including the close combination of intellectual property rights infringement crimes with cybercrimes, digital service software becoming new objects of infringement, most criminal subjects in cases of trade secret infringement being internal employees of enterprises, and insufficient evidence retention capability of infringed enterprises. In addition to the above "general" typological schemes, there are also some types that have a significant impact on the digital economy but are not positioned in an intermediate position and cannot serve as principal offenders of actionable behavior, such as advertising compliance (misconduct) and operational compliance (monopoly behavior). To enhance enterprises' ability to deal with criminal compliance risks, practical regulatory paths should be proposed: First, at the theoretical level, enterprise compliance management systems should be constructed, guided by incentive principles, principles of consistency between rights and obligations, and principles of systematic governance. Second, at the basic logical level, a multi-dimensional enterprise digital economy criminal compliance risk prevention should be achieved, through the construction of a criminal compliance digital platform, the strengthening of monitoring and early warning mechanisms, and supervision and evaluation mechanisms. Third, at the practical path level, regarding the object dimension of data security, a data classification and grading protection mechanism should be constructed and continuously optimized, the core responsibility system for enterprise data compliance should be established, and corresponding data compliance regulations should be improved; regarding the spatial dimension of cyberspace, enterprises' network security obligations should be clarified, and regular reviews and evaluations of network security compliance management systems and implementation mechanisms, as well as periodic evaluations of the work performance of network compliance management personnel, should be conducted; regarding the legal interest dimension of digital intellectual property rights, a comprehensive digital intellectual property rights compliance framework should be established, and enterprises should establish sound processes for digital intellectual property rights application, protection, and management, and actively utilize advanced technologies such as big data and artificial intelligence. Fourth, at the level of supporting management mechanisms, external supervision of digital compliance should be strengthened, digital criminal compliance legislation should be promoted, and collaborative governance of digital compliance should be facilitated. Through the regulatory paths of digital economy criminal compliance risks mentioned above, enterprises can gain advantageous positions in the process of digital economy development.

Key words: digital economy; data crime; criminal compliance; digital compliance