法学研究 Chinese Journal of Law
Vol.44，No.4（2022）

个人信息保护合规的体系构建

敬力嘉*

内容提要：作为企业管理工具，个人信息保护合规也存在被滥用的体系性风险。在分配个人信息处理风险时，应遵循比例原则的要求，合理限制公民个人、企业与国家公权力机关的个人信息处理自由，并以此作为个人信息保护合规的法理依据。企业在设计个人信息保护合规计划时，应遵循目的正当原则、区分原则、均衡原则与信赖原则。对企业进行个人信息保护合规审计时，应贯彻三阶审查法，即递进式审查合规计划的一般特征、具体要素及其功能、企业成员的具体行为。企业个人信息保护合规体系的底线，由侵犯公民个人信息罪划定。以企业的个人信息处理是否合规，以及企业领导人、合规负责人是否履行监管义务作为侵犯公民个人信息罪行为不法的评价标准，可有效保障本罪作为个人信息保护合规体系之底线的功能实现。

关键词：个人信息保护　企业合规　合规审计　侵犯公民个人信息罪

一、问题的提出

近年来，我国社会空间数字化水平大幅提升，企业处理个人信息可能引发的法益侵害风险愈加多样化。除了可能侵犯个人法益（如利用个人信息实施电信网络诈骗侵犯个人财产），也可能侵犯超个人法益。例如，国家网信办于2021年7月2日、7月5日对滴滴出行、BOSS直聘等进行网络安全审查后，〔1〕于2022年2月会同国家发改委等12个部委修订颁布了《网络安全审查办法》。该办法第7条、第8条规定，掌握超过100万用户个人信息的网络平台运营者赴国外上市，需申报网络安全审查，应提交关于影响或可能影响国家安全的分析报告。出台以上规定的目的，即在于防控大规模个人信息跨境流动所可能产生的国家安全风险。

在上述背景下，随着我国个人信息保护法律、法规、其他规范性文件以及技术标准与行业

* 武汉大学法学院副教授。

〔1〕 参见《我国已对滴滴BOSS直聘等启动网络安全审查》，https://wenhui.whb.cn/third/baidu/202110/10/427881.html，2022年1月7日最后访问。

规范体系的形成,〔2〕企业在经营中处理个人信息会面临显著的合规风险。在国内法方面,依据网络安全法第64条、个人信息保护法第66条至第68条、数据安全法第44条至第50条、“数据安全条例”第61条、第64条至第69条、“关键设施保护条例”第39条至第46条、“内容治理规定”第34条至第39条等有关规定,若企业违法违规处理个人信息,企业及相关责任人可能面临的处罚包括约谈、警告、罚款、计入信用档案、处分、限制或剥夺经营资格、从业禁止、没收违法所得与行政拘留。在个人信息流动周期内,企业处理个人信息也可能面临刑事处罚。〔3〕在外国法方面,欧盟《通用数据保护条例》(GDPR)第83条规定了高额行政罚款,各国网络治理领域的法律也对违法处理个人信息规定了行政和刑事处罚。与处罚相伴的声誉损失、商业机会损失等,〔4〕也都是需要考量的合规风险。因此,无论是以数据为核心生产资料的企业,还是利用信息网络开展业务的其他企业,个人信息保护合规都是企业运营的常态化要求,乃至企业上市审查的重要内容。〔5〕其不仅要求企业遵守非刑事个人信息保护法律法规,以及刑法第253条之一侵犯公民个人信息罪所创设的禁止性规范,还要求企业在前两者的基础上,以预防个人信息处理合规风险为目的确立管理要求。

当前对个人信息保护合规的研究,主要集中在对代表性企业合规业务模式的归纳、〔6〕APP隐私政策合规性的评估分析、〔7〕与GDPR合规要求的比较分析、〔8〕数据合规科技的风险规制、〔9〕数据合规语境下企业处理个人信息规范要求与数据保护官职能的梳理、〔10〕侵犯公民个人信息罪的保护法益与刑事责任认定〔11〕等六大方面。可以看到,既有研究主要着眼于梳理个人信息保护的规范要求、个案合规经验或法律责任判定,缺乏对个人信息保护合规这一企业治理机制的体系化省思。

以企业涉嫌违法犯罪为节点,可将企业合规分为事前自主合规与事后强制合规。〔12〕本文

〔2〕 我国个人信息保护法律体系以网络安全法、数据安全法、个人信息保护法为核心,法规体系以《网络安全保护等级条例(征求意见稿)》《网络数据安全管理条例(征求意见稿)》(以下称“数据安全条例”)《关键信息基础设施安全保护条例》(以下称“关键设施保护条例”)以及上海、浙江、深圳等省、市的数据条例为核心,其他规范性文件体系以《网络信息内容生态治理规定》(以下称“内容治理规定”)《互联网信息服务算法推荐管理规定》(以下称“算法推荐管理规定”)《网络安全审查办法》《互联网平台分类分级指南(征求意见稿)》(以下称“平台分类分级指南”)《互联网平台落实主体责任指南(征求意见稿)》(以下称“平台主体责任指南”)为核心,技术标准与行业规范体系以GB/T 35273-2020《信息安全技术 个人信息安全规范》(以下称“个人信息安全规范”)《网络安全标准实践指南——网络数据分类分级指引》(以下称“网络数据分类分级指引”)为核心。

〔3〕 参见敬力嘉:《单位犯罪刑事归责中数据合规师的作为义务》,《北方法学》2021年第6期,第103页以下。

〔4〕 参见陈瑞华:《企业合规的基本问题》,《中国法律评论》2020年第1期,第178页;李本灿:《企业视角下的合规计划建构方法》,《法学杂志》2020年第7期,第79页。

〔5〕 参见李哲:《政策监管出重拳,多款游戏APP涉侵犯隐私被下架处理》,《中国经营报》2021年9月6日B24版;宁宣凤、吴涵、包达等:《企业上市关注的重点数据合规问题》,《上海法学研究》(集刊)2020年第13卷,第263页以下。

〔6〕 参见陈瑞华:《中兴公司的专项合规计划》,《中国律师》2020年第2期。

〔7〕 参见肖雪、曹羽飞:《我国社交应用个人信息保护政策的合规性研究》,《情报理论与实践》2021年第3期。

〔8〕 参见王倩、顾雪莹:《GDPR下涉欧企业的员工个人数据合规管理》,《德国研究》2021年第2期。

〔9〕 See Christoph Burchard, *Digital Criminal Compliance*, in: Engelhart/Kudlich/Vogel (Hrsg.), Digitalisierung, Globalisierung und Risikoprävention: Festschrift für Ulrich Sieber zum 70. Geburtstag, Bd, II, 2021, S. 741-755.

〔10〕 参见相丽玲、王秀清:《中外数据保护官制度分析及启示》,《情报杂志》2021年第6期。

〔11〕 参见王肃之:《被害人教义学核心原则的发展——基于侵犯公民个人信息罪法益的反思》,《政治与法律》2017年第10期;欧阳本祺:《侵犯公民个人信息罪的法益重构:从私法权利回归公法权利》,《比较法研究》2021年第3期。

〔12〕 参见汪明亮:《作为犯罪治理方式的企业合规》,《政法论坛》2020年第3期,第177页;陈瑞华:《有效合规管理的两种模式》,《法制与社会发展》2022年第1期,第6页。

拟从企业事前自主合规的视角出发，探讨以下三个问题：第一，厘清个人信息保护合规的体系风险及法理依据；第二，明确个人信息保护合规计划的设计原则与有效性审查机制；第三，在个人信息保护合规体系中，明确侵犯公民个人信息罪所应具备的底线功能，并厘清实现该功能的具体路径。只有解答了以上三个问题，才能完成个人信息保护合规的体系构建。

二、个人信息保护合规的体系风险及法理依据

（一）个人信息保护合规的体系风险

作为一种企业管理工具，个人信息保护合规存在被滥用的风险。首先，从企业合规的一般属性看，“合规”（compliance）的词源（to comply）〔13〕已经揭示其“命令与控制”特征，“处罚不服从者”是其内在要求。不论是基于规范的合规，还是基于文化的合规，其“命令与控制”特征所潜藏的阴暗面在于，企业管理层可能滥用合规机制迫使员工不惜代价追求企业效益最大化，从而使合规机制成为企业系统性从事违法犯罪的理想工具。〔14〕美国富国银行（Wells Fargo）大规模私开账户的丑闻，便是适例。2015—2018 年，富国银行迫使其员工未经他人允许私开账户 350 余万个，并向被开户客户收取服务费，被开户客户的信用评级也因此受到影响。事发后，该银行开除了 5300 名员工，向美国消费者金融保护局缴纳了 1 亿美元罚款，向洛杉矶市检察官以及货币审计官办公室缴纳了 8500 万美元罚款。该银行拥有较完整的合规体系，包括详尽的合规指引、完备的合规组织架构与完善的合规程序。然而，该银行为部门经理和一般雇员设置了很高的业绩考核指标，并利用合规体系迫使其雇员不惜通过不法手段实现盈利目的。若有员工通过企业内部的吹哨人热线举报，企业合规负责人会将举报人名单通报给人力资源负责人，由后者以其他借口开除举报人。〔15〕

其次，具体到个人信息保护合规，由于当前个人信息处理多在信息网络环境下进行，个人信息保护合规与监控技术具有较高亲合度，存在以合规之名过度监控员工的风险。企业管理者易将员工视为可能引起处罚的潜在风险源，从而有较强动力以监管员工不法或不道德的个人信息处理行为为由，运用人脸识别、定位追踪、社交网络数据分析等手段尽可能多地搜集员工行为数据，以实现对合规风险的有效管控。而这可能导致企业管理者以信任监控技术取代信任员工，使合规管理去人性化，最终还可能侵犯员工合法权益。〔16〕例如，企业未履行“告知—同意”程序，在办公场所安装视频监控或人脸识别设备，安装电脑监控软件监控员工的电子邮件、社交媒体聊天记录等，以及为员工配备智能手环以监控其行踪轨迹，这些均可能侵犯员工的隐私权、个人信息权或其他正当权益。曾有美国公司通过综合运用人脸识别、定位追踪与社交网络数据分析等技术手段，准确预判了员工的离职意向，并将其提前解雇。〔17〕

（二）个人信息保护合规的法理依据

针对个人信息保护合规所存在的被滥用的风险，应进一步明确个人信息保护合规的法理依

〔13〕 See Brayan A. Garner (ed.), Black's Law Dictionary, 11th ed., Thomson Reuters, 2019, p. 357.

〔14〕 See J. S. Nelson, *Compliance as Management*, in: Benjamin van Rooij & D. Daniel Sokol (eds.), *The Cambridge Handbook of Compliance*, Cambridge University Press, 2021, pp. 104 – 118.

〔15〕 See M. Egan, *Wells Fargo Workers: I Called the Ethics Line and Was Fired*, CNN Money (September 21), http://money.cnn.com/2016/09/21/investing/wells – fargo – fired – workers – retaliation – fake – accounts, last visited on 2022 – 01 – 01.

〔16〕 参见前引〔9〕，Christoph Burchard 文，第 750 页以下。

〔17〕 参见前引〔14〕，Nelson 文，第 107 页。

据，以此作为管控风险、发挥合规治理效能的正当性根据。

民法与刑法学界的有力观点认为，个人信息保护的对象应为个人信息自决权。为了保护此项关涉公民人格尊严与发展自由的具体人格权，应以个人信息保护法第13条、第14条、民法典第1035条与网络安全法第41条为基础确立知情同意原则，并将其作为个人信息保护合规所应贯彻的一般性要求。〔18〕若遵循以上观点，保护个人信息自决权应为个人信息保护合规的法理依据。然而，个人信息保护法第5条规定的个人信息处理基本原则为“合法、正当、必要和诚信”，履行法定告知同意程序仅为形式合法性要件，并未否定对个人信息处理所关涉的其他主体正当权益或公共利益的保护。例如，前文列举的网络安全审查的有关规定，其目的即在于通过将大规模个人信息跨境流动纳入我国法律体系的规制范围，以保护国家安全。

再者，个人信息自决权首先是宪法层面的基本人权，其具体内涵有待进一步厘清。信息自决权概念来自德国，以1983年德国联邦宪法法院“人口普查案”为标志，创设了“在现代数据处理环境中，依据基本法第1条第1款（人的尊严不容侵犯）与第2条第1款（每个人都享有自由发展其人格的权利），公民个人数据不被无限制地搜集、存储、使用与转让”〔19〕的信息自决权。通过后续的系列判决，德国联邦宪法法院为信息自决权确立了符合显著公共利益、基于法律保留的合目的、透明、必要且合比例这四项基本原则。德国联邦宪法法院并未将信息自决权确立为公民对其个人信息的排他性控制支配权，而是将其确立为公民个人所享有、其个人信息不被不当处理的消极防御权。〔20〕随着时代发展，个人数据受保护权也体现了公民个人对其个人信息不被不当处理享有消极防御权的内涵。该项权利由欧盟《基本权利宪章》第8条第1款、《欧盟运行条约》第16条第1款以及GDPR立法理由第1条确立，对欧盟各国普遍适用。〔21〕在此基础上，民法理论发展出了作为具体人格权的个人信息权。〔22〕我国学者基本援引以上思路，并以我国宪法第38条、民法典第111条等相关规定为依据，证成了个人信息自决权应为我国法律保护的基本人权。〔23〕但是，若遵循这一思路，便不应主张个人信息保护合规的目的是保障公民对其个人信息积极的控制支配。个人信息保护合规的制度功能，应是平衡个人信息处理中个人与信息控制者非对称的权力结构，以实现对个人信息处理相关主体利益的妥善保护。〔24〕因此，个人信息保护合规的法理依据，应为个人信息处理潜在风险的合比例分配，其表现为对公民个人、企业与国家公权力机关个人信息处理自由的合理限制。

第一，知情同意原则存在显著局限性，这表明公民个人难以独自承担个人信息保护义务。在确立和完善个人信息保护立法的过程中，对知情同意原则的质疑始终不曾散去。〔25〕目前学界的主流观点认为，通过保障充分告知与实质同意、细化不同类型同意的规范内涵与法律效

〔18〕 参见程啸：《论我国个人信息保护法中的个人信息处理规则》，《清华法学》2021年第3期，第61页以下；刘艳红：《侵犯公民个人信息罪法益：个人法益及新型权利之确证——以〈个人信息保护法（草案）〉为视角之分析》，《中国刑事法杂志》2019年第5期，第27页以下。

〔19〕 BVerfGE 65，1（Volkszälungsurteil）.

〔20〕 BVerfGE 27，1，7-Mikrozensus；35，202，220-Lebach；54，148，155-Eppler；63，131，142-Gegendarstellung.

〔21〕 参见王锡锌：《个人信息国家保护义务及展开》，《中国法学》2021年第1期，第148页以下。

〔22〕 参见陈道英：《从德国法上的一般人格权看宪法权利与民事权利的协调》，《法学评论》2011年第5期，第61页以下。

〔23〕 参见前引〔18〕，刘艳红文，第30页以下；马永强：《侵犯公民个人信息罪的法益属性确证》，《环球法律评论》2021年第2期，第109页。

〔24〕 参见前引〔21〕，王锡锌文，第146页以下。

〔25〕 参见范为：《大数据时代个人信息保护的路径重构》，《环球法律评论》2016年第5期，第92页以下。

力、引入基于场景的风险管理与评估机制或其他多元规制机制等制度设计，可使知情同意原则摆脱困局。〔26〕这些措施对于优化知情同意原则具有重要意义，但仍无法突破知情同意原则保护效力的局限。这是因为，即使能让信息主体“充分知情、自主同意”，“理性信息主体”的假设也只是一种理想。已有学者指出，一般而言，公民个人的知情同意仅表明其知晓个人信息被处理，而非其充分衡量了个人信息处理的风险并愿意接受该风险。〔27〕行为决策心理学的研究更已证明，人的决策往往会出现系统性的非理性；即使具有充分的决策参考信息，人们通常也不会理性地考察整体决策树，而是会关注自己预先偏好选项的收益或损失，并最终作出决策；过度关注沉没成本，“锚定与调整”、启发式等常用的判断策略，即充分体现了人类行为决策理性的有限性。〔28〕因此，即使“算法推荐管理规定”第 8 条设置了防诱导机制，着力降低算法对公民个人选择偏好的影响，也仍然无法突破人类自身决策行为的局限。总之，仅依靠信息主体的知情同意，难以充分保障个人信息处理相关主体的权益。因此，应合理限制企业的个人信息处理自由，使国家能够通过合规机制保护相关主体（包括信息主体）的合法权益。

第二，为实现对个人信息的有效利用，应合理限制公民的个人信息处理自由，并通过合规机制稳定企业对“合理处理”个人信息自由空间的行为预期。数字经济时代，个人信息已成为相关企业必备的生产资料，平衡个人信息保护与合理利用需求已成为社会共识。对于如何实现这一平衡，学界主要有数据确权和行为规制两类观点。前者主张以民法典第 111 条、第 127 条对“个人信息”和“数据”的区别规定为规范基础，在为个人信息主体赋权的同时，将经过匿名化处理的个人信息视为非个人信息的企业数据，为作为企业数据控制主体的企业赋予财产权。后者则主张不为个人信息主体赋权，而是遵循场景化思路规制个人信息处理行为，保护信息主体与个人信息控制者的相关合法利益。〔29〕

2021 年 12 月，中央网络安全和信息化委员会印发了《“十四五”国家信息化规划》。〔30〕本文认为，若以《“十四五”国家信息化规划》提出的“数据治理”理念为指引，以个人信息保护合规为制度支撑，即可实现数据确权与行为规制两条路径的有效融合。质言之，以是否有效履行“告知—同意”程序作为企业处理个人信息合法性的判断标准，再以企业已履行个人信息处理的合规要求作为违法阻却事由的做法，〔31〕实属舍本逐末。而无论是对处理已公开个人信息行为进行合目的性考察，〔32〕还是以信息的客观开放程度为判断标准，对完全开放个人信息、限制开放个人信息与违法公开个人信息的处理赋予不同的规范要求，〔33〕对企业“合理处理”个人信息判断标准的界定也都不完整。直接以个人信息保护合规作为企业处理个人信息合法性的判断标准，可有效覆盖知情同意原则对信息主体个人权利的保护范围，以及个人信息保护法第 13 条中知情同意原则的例外情形。企业作为个人信息控制者，只要遵循处理不同类型

〔26〕 参见郭旨龙、李文慧：《数字化时代知情同意原则的适用困境与破局思路》，《法治社会》2021 年第 1 期。
〔27〕 参见高富平：《同意≠授权——个人信息处理的核心问题辨析》，《探索与争鸣》2021 年第 4 期，第 93 页。
〔28〕 参见［美］雷德·海斯蒂、罗宾·道斯：《不确定世界的理性选择——判断与决策心理学》，谢晓非、李纾等译，人民邮电出版社 2013 年版，第 19 页以下。
〔29〕 参见龙卫球：《数据新型财产权构建及其体系研究》，《政法论坛》2017 年第 4 期，第 65 页以下。
〔30〕 《“十四五”国家信息化规划》，http://www.cac.gov.cn/2021-12/27/c_1642205314518676.htm，2022 年 1 月 8 日最后访问。
〔31〕 参见周光权：《委托处理个人信息与侵犯公民个人信息罪——结合〈个人信息保护法〉第 21 条的分析》，《环球法律评论》2021 年第 6 期，第 32 页以下。
〔32〕 参见周光权：《侵犯公民个人信息罪的行为对象》，《清华法学》2021 年第 3 期，第 37 页，第 40 页。
〔33〕 参见王华伟：《已公开个人信息的刑法保护》，《法学研究》2022 年第 2 期，第 198 页以下。

个人信息的合规要求，其处理行为便属“合理”，应自始为法秩序所容许。

第三，为避免公权力恣意介入信息主体与企业的个人信息处理空间，应适用合规机制限制国家公权力机关的个人信息处理自由，以保障信息主体与企业的合法权益。一方面，为防止在信息社会治理中过度依赖监控技术，以监控取代信任、以监控置换自由，国家公权力机关应依据个人信息保护法第33条至第37条的规定，以保护公共安全作为适用监控技术的目的限定，谨守处理人脸信息等敏感信息时应遵循的规范要求。另一方面，在规范个人信息处理的法律框架中，国家公权力机关不仅是个人信息处理者，还是企业处理个人信息的监管者。当有关部门履行个人信息保护法第61条规定的个人信息保护职责时，应避免逾越权限妨害企业经营自由或其他合法权益。

三、个人信息保护合规计划的设计原则与有效性审查

在“数据治理”理念的指引下，明确个人信息保护合规的法理依据是合比例分配个人信息处理的潜在风险，其最重要的意义是立足于个人信息流动的现实过程，厘定个人信息保护的责任主体应是作为个人信息控制者的企业和国家公权力机关，而非公民个人。本文不拟探讨国家公权力机关的个人信息保护合规问题，而仅以前文确立的法理依据为基础，进一步确立企业个人信息保护合规计划的设计原则与有效性审查机制。

（一）个人信息保护合规计划的设计原则

应当明确的是，《企业境外经营合规管理指引》（以下称“境外经营合规指引”）第5条确立的独立性、适用性、全面性原则过于宽泛，无法明确指引具体的制度设计，而个人信息处理应当遵循的“合法、正当、必要和诚信”原则，又不以规范企业组织管理为目的，因而也无法适用。本文不拟赘述合规计划应具备的共性要素，而只着眼于厘清个人信息保护合规计划的设计原则，以及贯彻相应设计原则的重点要求。

第一，目的正当原则。首先需要指出，个人信息保护合规目的不同于个人信息处理目的。前者指引企业对个人信息保护合规计划的设计，后者则约束企业的个人信息处理行为。具体而言，事前自主合规的目的是完善公司管理体系，预防合规风险。事后强制合规则主要指刑事领域内企业在合规考察期的强制整改，其目的不是预防合规风险，而是通过合规整改消除企业再犯风险；可将其视为针对企业的刑罚替代措施，体现了特殊预防目的，相应处罚措施则是对企业犯罪行为不法的报应。〔34〕就个人信息保护事前自主合规而言，企业需识别不同个人信息处理参与形式所代表的合规风险分配方式，将协议风控作为个人信息保护合规计划的重要内容，如此才能实现有效预防合规风险的目的。

关于个人信息处理的参与形式，现实中多方主体参与个人信息处理是常态，参与形式主要包括共同处理、委托处理、独立主体间的合作处理，个人信息保护法第20条至第23条对此作了规定。根据个人信息保护法第73条第1项的规定，“个人信息处理者”是指可以自主决定处理目的与方式的组织和个人，其内涵等同于GDPR语境下的“个人数据控制者”。〔35〕依据

〔34〕 Vgl. Markus Wagner, Besonderheiten der Criminal Compliance im Vergleich zur nichtstrafrechtsbezogenen Compliance, in: Rotsch (Hrsg.), Criminal Compliance-Status quo und Status futurus, 2021, S. 451.

〔35〕 参见程啸：《论个人信息共同处理者的民事责任》，《法学家》2021年第6期，第18页以下。

GDPR 第 26 条的规定，能够共同决定个人数据处理目的与手段的，属于个人数据的“共同控制者”。依据欧洲法院作出的三项代表性判决，〔36〕在不同阶段介入的个人数据处理者，只要对处理的目的与手段具备决定性影响，就是“共同控制者”。受委托处理个人数据者无权决定“是否”以及“如何”处理个人数据，不属于“控制者”，其只是 GDPR 第 4 条、第 28 条规定的“处理者”。〔37〕我国个人信息保护法不区分“控制者”和“处理者”，GDPR 语境下的“处理者”，应与个人信息保护法第 21 条规定的受托处理者具有同等内涵。区分个人信息处理参与形式的意义不仅在于认定民事侵权责任，更在于确认合规风险的分配方式。前两种参与形式下，可以个人信息处理参与主体有关权限分配的共同约定为基础，根据各自对个人信息处理造成侵害的实际贡献，将合规风险合理分配给共同处理者、委托处理者和受托处理者。独立主体合作处理个人信息时，合作的个人信息处理者应独立承担合规风险。

随着工信部、市场监管总局等部门专项整治行动的展开，以及《禁止网络不正当竞争行为规定（征求意见稿）》、“平台分类分级指南”“平台主体责任指南”的出台，我国网络平台的互联互通是否以及如何影响个人信息处理的参与形式，值得特别关注。在目前的外链开放阶段，各平台独立处理个人信息并评估、承担相应合规风险仍属常态，企业应根据不同参与形式评估个人信息处理的合规风险并对风险进行合理分配。以网络爬虫技术为例，已有学者指出，“robot 协议”“user-agent”“device id”“IP 地址”等技术性措施无法验证计算机信息系统登录权限，不应将这些措施认定为安全防护措施，规避以上措施的爬取行为不应构成非法获取计算机信息系统数据罪。〔38〕本文赞同此观点。笔者认为，应慎用刑法规制爬取公开个人信息的行为，可将其视为数据互通的先期探索，并考虑将爬取公开个人信息者视为共同处理者，令其承担处理公开个人信息的合规风险，进而赋予其“合理处理”的合规义务。

根据个人信息处理的不同参与形式，企业应注重协议风控体系的建设，约定与合作伙伴或供应商共同处理、委托处理、独立主体间合作处理的权限分配，奠定合规风险分配的基础。在这一方面，中兴公司的数据保护合规体系较为成熟，具备较高的参考价值。该公司设置了专职数据保护官，确立了“政策、手册、原则性规范、场景化指引”的规则架构，以识别公司运营中的数据保护风险。以此为基础，该公司集中推动与各相关方建立数据保护协议风控体系，建立了完整的数据合规培训与考评体系，将数据合规要求融入具体商事活动流程，着力避免企业日常经营中由个人信息处理诱发的合规风险。〔39〕

第二，区分原则。企业合规计划不应贪大求全，应在参照合规管理标准的基础上，根据企业实际情况与具体需求进行个别化设计，如此才能激活书面合规计划的效力。然而，确立专项合规计划的要求还是太过宽泛，需要进一步研究如何实现专项合规计划的个别化设计。落实到个人信息保护合规计划，需在设计中遵循区分原则。

首先，应区分企业类型。企业类型不同，对个人信息保护合规的需求显著不同。个人信息

〔36〕 三项判决分别认定了三组相应个人数据的共同控制者：脸书粉丝页管理者与作为平台运营者的脸书、宗教组织与承担传教职能的组织成员、社交网站运营者与社交插件提供者。Vgl. EuGH NJW 2018, 2537（2538）Rn. 25 ff.; EuGH NJW 2019, 285（289f.）; EuGH, Urt. v. 29. 7. 2019-C 40/17.

〔37〕 参见 Jörg Eisele, Sonja Kreß, Criminal Compliance und Datenschutz-Grundverordnung, 载前引〔34〕, Rotsch 编书, 第 100 页以下。

〔38〕 参见孙禹：《强行爬取公开数据构成犯罪吗》，《国家检察官学院学报》2021 年第 6 期，第 126 页以下。

〔39〕 参见 ZTE 中兴：《数据保护合规》，https://www.zte.com.cn/china/about/trust-center/Legal-and-Compliance/201901230922.html，2022 年 1 月 15 日最后访问。

密集型企业控制了大量个人信息，或其商业模式对个人信息有较大需求，属于个人信息保护法律规范体系的重点规制对象。对此类企业而言，无论是以个人信息为核心生产资料的互联网企业与大数据交易所，还是利用信息网络开展业务的金融、物流、汽车、教育、健康医疗等行业企业，一旦在个人信息处理中发生违规事件，处罚风险以及连带的经济、声誉与商业机会损失等均难以估量。例如，在2018年脸书用户数据大规模泄漏，导致其声誉严重受损、股价大跌之后，2022年1月脸书又因未允许法国用户便捷拒绝cookie跟踪，被法国的数据监管机构处以6000万欧元罚款。〔40〕有效的个人信息保护合规计划是此类企业健康发展的重要保障，属于企业核心竞争力的组成部分，非个人信息密集型企业则无需为个人信息保护合规计划投入过多资源。此外，根据“关键设施保护条例”第2条的规定，属于关键信息基础设施运营者的企业，对个人信息保护合规计划的需求显著强于一般个人信息处理者。

其次，应区分企业规模。美国市场调查公司的研究报告预测，2030年全球风险与合规产业的市场总值将达到1348亿美元。〔41〕随着企业合规制度在我国全方位落地，我国企业合规市场也将向资金投入与从业人员数量快速攀升的方向发展。鉴于合规成本基本由企业承担，依据不同规模企业的经济能力制定个人信息保护合规计划，便成为设计企业合规计划的应然要求。“平台分类分级指南”和“平台主体责任指南”对互联网平台经营者数据合规的区分规定，较好地体现了这一要求。比如，依据“平台分类分级指南”，互联网平台经营者可分为超大型、大型与中小型平台；不同于“平台主体责任指南”第18条、第24条至第27条为网络平台规定的一般性数据合规义务，“平台分类分级指南”第4条至第8条赋予了超大型平台经营者更为严格的数据合规体系建设义务。

第三，均衡原则。正如前文所指出，个人信息保护合规的法理依据是，以合比例分配个人信息处理的潜在风险为目的，对公民个人、企业与国家公权力机关的个人信息处理自由进行合理限制。因此，个人信息保护合规应属于对企业处理个人信息的公私合作治理机制，其应受比例原则的规制。在比例原则的四项子原则中，个人信息保护合规计划的目的正当性与合规措施的必要性，已分别融入前文确立的目的正当原则和区分原则。合规措施的适当性，要求检验个人信息保护合规计划的有效性，下文将展开进一步探讨。均衡原则则要求合规措施带给企业的负担应与其目的相均衡，这要求个人信息保护合规计划应避免创设过多的、不必要的复杂合规规则，否则会让企业难以完成合规要求，让合规陷入形式主义、官僚主义困局。

针对不同类型个人信息的重要性，为企业创设与之相匹配的合规要求，是在个人信息保护合规计划设计中贯彻均衡原则的应然之义。关于个人信息的类型，主要有以下三种分类标准：（1）以个人信息的法益关联性为标准，可分为敏感个人信息和非敏感个人信息。敏感个人信息可直接关联公民的人身或财产法益，其重要性显著高于非敏感个人信息。“网络数据分类分级指引”6.4.2条即以此为标准，对个人信息进行了更加细致的定级。（2）以个人信息的可识别性为标准，可分为匿名化个人信息和非匿名化个人信息。依据个人信息保护法第2条的规定，匿名化个人信息不属于本法规制的对象。考虑到重新识别技术的存在，企业难以绝对保障个人信

〔40〕 参见新浪科技：《谷歌和Facebook在法国面临隐私权相关巨额罚款》，https://baijiahao.baidu.com/s?id=1721157540813138730&wfr=spider&for=pc，2022年1月15日最后访问。

〔41〕 See *Enterprise Governance, Risk & Compliance Market Worth $134.8 Billion by 2030*, Grand View Research (April 2022), www.grandviewresearch.com/press-release/global-enterprise-governance-risk-compliance-egrc-market, last visited on 2022-04-13.

息匿名化处理后“无法识别”与“不能复原”。在企业掌握足够多与个人有关数据的场合，“个人信息安全规范”3.14 条规定的个人信息去标识化也可以被逆转。因此，应在个人信息处理的具体场景中，根据个人信息的重标识风险（识别难度）、企业掌握与个人有关数据的丰富程度及其技术能力，判断匿名化个人信息的重要性。〔42〕（3）以个人信息的可获取性为标准，可分为公开个人信息和非公开个人信息。个人信息的公开范围越小，原则上该信息越重要。但是，对公开个人信息的处理若违反个人信息保护法第 27 条的“合理处理”要求，也可能受到行政处罚，还可能因“违反国家有关规定向他人出售或提供公民个人信息”而构成侵犯公民个人信息罪。〔43〕因此，在企业的个人信息保护合规计划中，应确立与个人信息重要性相匹配的合规要求，避免给企业带来过重负担。例如，依据个人信息保护法第 23 条、第 25 条、第 26 条、第 29 条、第 39 条以及“数据安全条例”第 21 条的规定，企业处理相应个人信息时，需就个人信息类型、处理目的、方式等取得个人的单独同意。在具体落地为对企业的个人信息保护合规要求时，如何确保可操作性，不给企业增加过重负担，是今后有待进一步研究的课题。此外，均衡原则也要求个人信息保护合规计划的设计应注意与现有规范相衔接，如无必要，勿增设新的合规义务。

第四，信赖原则。个人信息保护合规措施具有强制性，且与技术监控手段具备高亲合度。这一特征不仅极易导致过度合规，从而侵犯企业员工合法权益，而且会对员工发出不信任信号，致使员工抗拒个人信息保护合规的管理要求，侵蚀员工对企业的信任感、归属感和责任感。在设计个人信息保护合规计划时，应避免对员工的有害推定，并将员工个人信息纳为合规计划的保护对象。

目前，已有学者关注到职场中监控技术的广泛应用，及其对普通劳动者个人信息权的不当侵害，并从国家视角出发，提出了完善劳动者个人信息法律保护的基本原则和专门进路。〔44〕本文提出的信赖原则就是从企业视角出发，要求企业在数字化经营管理活动中谨守对员工的无害推定，实现对其个人信息的妥善保护。随着算法在金融、医疗、汽车等各行业领域的广泛应用，其已经成为数字经济时代企业管理的重要技术支撑。在数字化的经营管理活动中，企业可利用以算法为核心的智能管理系统收集海量员工个人信息，并对其进行自动化处理。例如，我国大型互联网公司广泛使用员工行为感知检测系统，实现对员工离职倾向的分析以及更为广泛的行为监控，并在此基础上对员工进行考核乃至解聘。〔45〕而目前有关算法规制的研究多从国家视角展开，着眼于用户权利配置和算法规制法律框架的设计，〔46〕未充分重视对算法应用主体的行为规制。〔47〕本文认为，为了在个人信息保护合规计划中贯彻信赖原则，避免企业将责任推卸给算法，有效约束企业利用算法处理员工个人信息的行为，应接纳算法的“黑箱”属

〔42〕 参见叶小琴、王肃之、赵忠东：《大数据时代公民个人信息可识别性认定模式的转型》，《法治社会》2021 年第 6 期，第 27 页以下。

〔43〕 参见刘双阳：《“合理处理”与侵犯公民个人信息罪的出罪机制》，《华东政法大学学报》2021 年第 6 期，第 60 页以下。

〔44〕 参见王倩：《作为劳动基准的个人信息保护》，《中外法学》2022 年第 1 期。

〔45〕 参见钟艺璇：《大厂监控风云》，https://baijiahao.baidu.com/s?id=1724886770495047555&wfr=spider&for=pc，2022 年 4 月 13 日最后访问。

〔46〕 参见王莹：《算法侵害类型化研究与法律应对——以〈个人信息保护法〉为基点的算法规制扩展构想》，《法制与社会发展》2021 年第 6 期。

〔47〕 参见金梦：《立法伦理与算法正义——算法主体行为的法律规制》，《政法论坛》2021 年第 1 期，第 35 页以下。

性，通过个人信息保护合规机制的设计，使算法对个人信息的处理满足可检验与审计、受协议约束、保留人工权限等要求。〔48〕通过欧盟式 Gaia-X 云平台推行个人信息保护合规，〔49〕是一个值得借鉴的方案，而这有赖于国家数据治理技术基础设施建设的进一步完善。

（二）个人信息保护合规计划有效性的审查机制

在厘定了个人信息保护合规计划的设计原则之后，还应进一步考察合规计划有效性的审查机制。目前，质量认证是判断企业合规计划有效性的通行思路，即以有效合规计划构成要素是否完备，以及发生违规或违法犯罪行为时企业是否遵循合规计划要求，作为企业合规计划是否有效的判断标准。〔50〕作为判断依据的有效合规计划构成要素，出自《中央企业合规管理指引（试行）》（以下称“央企合规指引”）“境外经营合规指引”以及 GB/T 35770－2017《合规管理体系指南》等合规管理标准。但是，企业合规计划的效力，并不是在合规计划制定与执行后就能得到稳定保障。以刑事领域的事后强制合规为例，目前欧美学界有经验研究支持“涉案企业充分遵循了暂缓起诉（DPA）或不起诉协议（NPA）要求”的结论，也存在适用企业合规管理措施后被起诉次数减少的个案研究。但企业适用合规管理措施后被起诉次数减少的原因，也可能并不是相关协议对企业犯罪产生了预防效果，而是适用相关协议后，检察官可以不再证明具体涉案企业或责任人的刑事责任。目前，暂无经验证据能直接证明“暂缓起诉或不起诉协议具有减少企业犯罪效果”的结论。〔51〕

在企业合规计划的具体执行中，企业员工对合规计划的认同与接受程度，也能在很大程度上影响合规计划实际发挥的效果。在社会网络分析的理论视角下，企业的制度、规范、文化，包括合规计划确立的行为规范，更像一个可供选择的工具箱，而非约束行为的静态规则系统。“它们影响（塑造）行为，但不决定行为，人们在解决问题的时候，往往会实践性地选择指引规则，而不在意它们的体系性。”〔52〕即使企业制定了足以通过质量认证的完善合规计划，在具体实施过程中，其实际效果也可能由于合规负责人执行意愿或执行能力不足，或企业中下层员工之间形成应付合规管理措施的潜规则、小团体而大打折扣。此外，合规人员也可能在公司内部被孤立。而行业联盟设立的合规准则，对于确保企业合规计划执行效果的作用也较为有限。因为企业领导层遵循合规要求的动机往往不是认可这些行为准则，而是因为合规可以为企业带来经济效益。企业愿意承担合规成本，一定是以创造效益为前提的。〔53〕

因此，质量认证式的检验，只能判断企业合规计划的适格性而非有效性。已有检察机关实务工作者认识到以上问题，试图将以企业文化为核心的合规免疫系统作为合规计划有效性的评

〔48〕 参见 Janique Brüning, Künstliche Intelligenz und strafrechtliche Haftung-Compliance-Anforderungen im digitalen Zeitalter mit Blick auf die Finanzwirtschaft, 载前引〔34〕, Rotsch 编书, 第 83 页以下。

〔49〕 各利益相关方接入 Gaia-X 基于云架构的公共数据空间，根据合规标准的差异，Gaia-X 定义了三个标签级别：级别 1（基础合规）、级别 2（实质合规）、级别 3（高度合规）。根据特定服务属性指定标签，平台自动测试特定服务并发放标签，以标识相关服务的合规水平。https://gaia－x. eu/sites/default/files/2021－11/Gaia－X%20Labelling%20Framework_0. pdf, last visited on 2022－04－13.

〔50〕 参见孙国祥：《企业合规改革实践的观察与思考》，《中国刑事法杂志》2021 年第 5 期，第 34 页；陈瑞华：《企业合规不起诉改革的八大争议问题》，《中国法律评论》2021 年第 4 期，第 25 页以下。

〔51〕 参见 Melissa Rorie & Natalie Schell-Bussey, *Corporate Crime Deterrence*, 载前引〔14〕, Benjamin van Rooij 等编书, 第 223 页以下。

〔52〕 前引〔3〕，敬力嘉文，第 101 页。

〔53〕 参见 Ralf Köbel, Kriminologisch-empirische Forschung zu Criminal Compliance, 载前引〔34〕, Rotsch 编书, 第 145 页以下。

价标准，并确立了具体的技术指标、文化指标以及多元检测模型。〔54〕这已向合规计划有效性评价标准的革新迈出了重要一步，但尚未彻底完成从倚重静态质量认证向构建全过程动态审查的企业合规计划审查机制的转型。对此应作进一步分析。

具体到个人信息保护合规，应以个人信息保护法第 54 条、第 64 条、“平台主体责任指南”第 8 条规定的事前合规审计为制度依托，对合规计划进行三阶过滤式审查，以确认其有效性。第一步，应审查个人信息保护合规计划的一般特征。在这一阶段，应确定企业所属行业、类型、规模大小，根据前文提出的合规计划设计原则确定合规计划的具体内容和复杂程度，审查合规计划是否对企业面临的个人信息处理合规风险具备针对性。第二步，应审查个人信息保护合规计划的具体要素及其功能。在这一阶段，不能由单一要素不具备或者运行不规范，就得出合规计划无效的结论，而应全面检验企业合规体系对违规或违法处理个人信息行为的预防、揭露与反应功能，着重检验企业的吹哨人机制、举报信息处理机制与内部调查机制。第三步，应在行为合规的语境下审查企业成员的具体行为。为了不让个人信息保护合规沦为企业的格式化装饰或者企业规训员工的工具，就不能忽略人的因素。个人信息保护合规计划的目的不是为企业卸责，而是改变企业的文化基因，让企业成员不想违规或违法犯罪。应当塑造激励员工道德感与责任感的企业文化，加强对具体的人的行为规范的塑造与考察。〔55〕

（三）个人信息保护合规审计

目前，我国已有两部个人信息保护合规审计评估标准的指引性文件，即《个人信息处理法律合规性评估指引》（T/CLAST 002.1－2021）（以下称“合规性评估指引”）〔56〕和《关于推进个人信息保护合规审计的若干建议》（以下称“合规审计建议”）〔57〕。二者分别由中国科学技术法学会、中国信息通信研究院云计算与大数据研究所牵头，多家代表性企业共同参与制定。这体现了业界对于厘定个人信息保护合规审计规范定义与审计内容的迫切需求，但学界对此缺乏必要的理论关注。

在展开具体探讨前，需先厘清“个人信息保护合规审计”的规范内涵。在我国现行规范体系内，“境外经营合规指引”第 26 条直接使用了“合规审计”概念，法律法规层面只有个人信息保护法第 54 条、第 64 条使用了这一概念。审计学视域下，合规审计是判断特定行为是否符合既定标准（包括法律规范和合约要求），并将结果传递给利益相关者的一种审计模式。〔58〕个人信息保护合规审计，是对企业的个人信息处理行为是否符合既定标准的判断。“合规性评估指引”和“合规审计建议”均遵循这一理解，针对个人信息处理的不同环节确立了行为合规性的判断标准。与“央企合规指引”第 20 条规定的“合规审查”相比，个人信息保护合规审计要求设置特定的审计程序；与 GB/T 20945－2013《信息安全技术 信息系统安全审计产品技术要求和测试评价方法》3.2 条规定的“安全审计”相比，个人信息保护合规审计的内容

〔54〕 参见李勇：《涉罪企业合规有效性标准研究——以 A 公司串通投标案为例》，《政法论坛》2022 年第 1 期，第 137 页以下。

〔55〕 参见 Juan Pablo Montiel, Carolina Boehler, Eignungstest für Compliance-Systeme und das Drei-Filter Modell, 载前引〔34〕，Rotsch 编书，第 221 页以下。

〔56〕 参见中国科学技术法学会：《个人信息处理法律合规性评估指引》，http://www.ttbz.org.cn/Pdfs/Index/?ftype=st&pms=56497，2022 年 4 月 13 日最后访问。

〔57〕 参见个人信息保护合规审计推进小组：《关于推进个人信息保护合规审计的若干建议》，http://www.chuangze.cn/third_down.asp?txtid=4567，2022 年 4 月 13 日最后访问。

〔58〕 参见郑石桥、李媛媛：《合规审计重要性：一个逻辑框架》，《商业会计》2017 年第 3 期，第 20 页。

更广泛。个人信息保护法第54条、第64条分别规定了作为日常合规管理措施的个人信息保护合规审计，与作为企业自主合规整改措施的个人信息保护合规审计。除了启动审计工作的动因和时间不同，二者具体的审计内容也存在实质区别。

个人信息保护法第54条要求企业定期进行的个人信息保护合规审计，其内容是审查个人信息保护合规计划的针对性，即前文提出的三阶审查法中第一阶段的审查。在审查个人信息保护合规体系的完整性时，应重点考察合规计划是否明确了个人信息处理权限与合规负责人监管权限。依据公司法第46条、第108条的规定，董事会应独立承担对公司的集体领导义务，包括合规管理义务。依据公司法第49条、第53条、第54条、第147条的规定，以相互承担对对方不法决定的监督、控制、干预义务为前提，董事会的领导职责可通过董事会成员间的水平授权，或公司内部、公司与合作伙伴间的垂直授权进行合理分配。但是，领导义务的核心，即对公司决策的决定与控制则不可分配。〔59〕换言之，明确个人信息处理与合规监管的权限，是确立个人信息保护合规计划的应然目的。只有如此，才能厘清影响企业决策的信息传递结构，以及判断企业的合规体系能否有效打破这一结构，从而阻断个人不法行为上升为企业不法行为。“合规性评估指引”5.11.2条设置的合规管理体系指标，以及“合规审计建议”第三章第一节“个人信息处理者义务合规审计”，都已涉及对以上内容的审查，今后可进一步遵循区分原则，实现相关审计要求的个别化。对于个人信息保护合规计划内容的完整性和针对性，可通过个人信息保护政策检测法、数据泄露事件汇总法、关键要素检测法等进行审查。〔60〕

个人信息保护法第64条要求的个人信息保护合规审计，则是对企业个人信息保护合规计划有效性的完整审查。履行个人信息保护职责的部门需要通过这样的审查，才能确认个人信息保护法第51条、第52条、第58条对个人信息处理者提出的合规管理要求的执行情况，并对企业的个人信息保护合规计划提出有针对性的整改措施。对此，需依照前文提出的三阶审查法，过滤式审查个人信息保护合规计划的一般特征、具体要素、应对违规或违法处理个人信息行为的功能，以及具体企业成员行为的合规性。第一阶段的审查内容和程序，应与个人信息保护法第54条规定的定期审计相同。在第二阶段对举报信息处理机制与内部调查机制有效性的检验中，不能忽视对员工个人信息保护情况的审查，并且需将此作为衡量个人信息保护合规计划功能的重要指标。〔61〕在第三阶段，飞行检查、对员工的不定期匿名访谈等措施，都能有效促进企业文化的改善。此外，监管部门对个人信息保护法第64条的适用，应严格遵循法定权限与程序，避免赋予企业过重的合规审计义务。

在吸收“合规性评估指引”和“合规审计建议”等既有文本有益经验的基础上，经过个人信息保护法实施后的实践探索，今后应考虑进一步确立个人信息保护合规审计的国家标准，以合理限制国家公权力机关对企业个人信息处理自由的介入。

四、个人信息保护合规的底线确立与保障

我国个人信息保护合规的规范依据具备鲜明的二元层次化特征，其不仅包括非刑事个人信

〔59〕 Vgl. Wabnitz/Janovsky/Schmitt (Hrsg.), Handbuch Wirtschafts- und Steuerstrafrecht, 5. Aufl., 2020, S. 372 – 379.

〔60〕 参见朱敏杰、叶青青、孟小峰等：《基于权限的移动应用程序隐私风险量化》，《中国科学：信息科学》2021年第7期，第1102页以下。

〔61〕 参见前引〔59〕，Wabnitz等编书，第405页以下。

息保护法律规范，还包括侵犯公民个人信息罪所创设的禁止性规范。立足于我国的“违法—犯罪”二元区分体系，个人信息保护法并未创设保护个人信息的附属刑法条款。基于刑法的保障法属性，在厘定了个人信息保护合规计划的设计原则与有效性审查机制之后，还需确立侵犯公民个人信息罪为企业个人信息保护合规体系划定的底线。通过明确本罪行为不法的评价标准，可保障该底线功能的实现。

（一）底线确立：侵犯公民个人信息罪的制度功能

侵犯公民个人信息罪是保护我国公民个人信息的基础性罪名，在民法典和个人信息保护法生效前后，本罪法益的确定，〔62〕以及本罪适用中刑法与前置法的衔接机制，〔63〕成为刑法学界的研究热点。然而，既有研究大多基于各自理论预设探讨个罪法益与刑事归责，难以形成有效对话。导致这一状况的根本原因是，既有研究未在个人信息法律保护的整体框架中明确本罪的制度功能。正如前文所指出，整体法秩序保护个人信息的规范目的是通过个人信息保护合规，合理限制公民个人、企业与国家公权力机关的个人信息处理自由，合比例分配个人信息处理的潜在风险，进而实现对个人信息处理所涉利益的妥善保护。侵犯公民个人信息罪针对个人信息处理行为所创设的禁止性规范，也是企业制定个人信息保护合规计划的重要依据。基于本罪保护法益的超个人属性，可以确立本罪为个人信息保护合规体系所划定的底线。

关于侵犯公民个人信息罪的保护法益，主要有个人法益和超个人法益两派观点。个人法益论的观点中，最有力的是个人信息自决权说。本文则持法定主体信息专有权说；该说属于超个人法益论的观点，认为本罪保护的法益是个人信息控制主体基于信息主体授权，及前者基础上的法定授权范围，处分所控制的个人信息的权限。在企业作为个人信息控制主体时，承载本罪法益的对象应为企业的个人信息保护合规机制。〔64〕本文不拟涉入具体论争，只拟基于以上观点证成侵犯公民个人信息罪在个人信息保护合规体系中的制度功能。

主张侵犯公民个人信息罪的保护法益是个人信息自决权的学者倾向于认为，本罪的行为对象是纯粹的、具有明确识别性的个人信息，其具有强烈的个人信息自决属性，不容他人侵犯。〔65〕该观点对个人信息的理解脱离了个人信息的形成过程，人为割裂了个人信息与个人数据的内在关联。事实上，所谓个人数据，是标准化、可再处理的个人信息表达形式，是个人信息内容的荷载符号。通过处理个人数据，可以获得有效个人信息。而且，个人信息不是静态存在的客体，而是在不同主体控制个人数据的交换中产生的“意义”，或者说内容。个人信息的“个人”属性，只能依托于数据交换过程而存在。正因如此，个人信息处理关涉的利益多样，不限于个人信息权利，还包括他人权利乃至公共利益。

主张侵犯公民个人信息罪的保护法益是个人信息自决权的观点，也脱离了个人信息保护法与个人信息保护合规的整体架构，仅在公民个人与国家二元对立的传统结构中展开探讨。基于此，自然可轻易得出“刑法对公共价值的保护仅具有衍生性定位，对个人信息公共价值的挖掘不能逾越个体权利”的结论，进而将本罪解释为保护个人法益的犯罪。〔66〕但正如前文所

〔62〕 参见姜涛：《新罪之保护法益的证成规则——以侵犯公民个人信息罪的保护法益论证为例》，《中国刑事法杂志》2021 年第 3 期；前引〔11〕，欧阳本祺文。

〔63〕 参见前引〔31〕，周光权文；前引〔43〕，刘双阳文。

〔64〕 参见敬力嘉：《信息网络犯罪规制的预防转向与限度》，社会科学文献出版社 2019 年版，第 101 页以下。

〔65〕 参见前引〔23〕，马永强文，第 104 页。

〔66〕 同上文，第 110 页以下。

述，个人信息自决权是作为公民基本权利的消极防御权，而非积极控制支配权。若以数据治理为基本理念，以法定主体的信息专有权作为本罪的保护法益，则应将本罪理解为保护超个人法益的犯罪。如此，可通过保护企业的个人信息保护合规机制，实现对个人信息处理关联主体权益，包括公民个人信息自决权的前置保护。总之，本罪在个人信息保护合规体系中的制度功能是确保企业贯彻目的正当原则的要求，以预防合规风险为目的确立个人信息保护合规机制并保障其效力，且以此作为企业个人信息保护合规体系的底线。只有这样，才能有效激励企业切实履行个人信息保护职责，实现个人信息合规利用与个人信息妥善保护的权责统一。

（二）底线保障：侵犯公民个人信息罪行为不法的评价标准

基于以上认识，通过明确在企业成立侵犯公民个人信息罪的场合，企业、企业领导人与个人信息保护合规负责人行为不法的评价标准，可进一步保障在个人信息保护合规体系中侵犯公民个人信息罪所承担的底线功能的实现。

1．企业行为不法的评价标准

前述主张以个人信息自决权为保护法益的观点认为，应以是否经公民个人知情同意作为侵犯公民个人信息罪行为不法的判断标准，并且此知情同意即为刑法中的被害人同意，可以阻却违法；若同意违背对公共价值的保护需求，则不能阻却违法。〔67〕但是，如前文所指出，信息主体常常不明知个人信息处理行为的潜在风险，其同意权限和同意能力更是无从谈起。因此，信息主体“知情同意”中的同意，并不属于刑法中的被害人同意。进而，以信息主体的知情同意作为阻却违法的正当化事由，自然就不具备充分理据。

依本文所持观点，在企业成立侵犯公民个人信息罪的场合，其个人信息保护合规机制是承载本罪法益的对象。信息主体是否知情同意，仅是个人信息处理合规的形式要件之一，而非唯一要件。因此，应以个人信息处理是否合规作为企业行为不法的判断标准。对于个人信息处理是否合规，则需根据企业事前自主确立的个人信息保护合规计划进行审查。遵循以上归责进路，可实现刑法规范与前置法规范的有效衔接，保障企业个人信息保护合规体系的底线不失守。以“淘宝商铺信息转让案”为例，〔68〕已经取得信息主体同意的信息倒卖者宋某某等构成侵犯公民个人信息罪的理由，并不是违背所谓社会交往利益，从而使被害人同意无法阻却违法，而是由于其贩卖公民个人信息的行为不合规，进而证成其行为的刑事不法。需要特别注意的是，依据个人信息保护法第 64 条第 2 款的规定，在对企业个人信息保护合规计划有效性进行完整审计的过程中，若履行个人信息保护职责的部门发现违法处理个人信息涉嫌犯罪的，应及时移送公安机关依法处理。这意味着，该规定要求的个人信息保护合规审计，可为侵犯公民个人信息罪发挥底线功能提供常态化的制度保障。

2．企业领导人、合规负责人行为不法的评价标准

在企业成立侵犯公民个人信息罪的场合，还需厘清企业领导人、个人信息保护合规负责人行为不法的评价标准。只有如此，才能明确二者应承担的具体监管义务，发挥本罪创设的行为规范对二者的激励效果，有效保障个人信息保护合规体系的底线不失守。

目前，国内学界对以上问题仅作了相当有限且较为宽泛的探讨。认可二者应对企业雇员实施的、具备业务关联性的犯罪行为承担监管义务的观点，多通过认可二者的保证人地位来证成

〔67〕 参见前引〔23〕，马永强文，第 113 页以下。

〔68〕 参见广东省开平市人民法院（2018）粤 0783 刑初 215 号刑事判决书。

其监管义务。反对观点主要认为，在我国刑法存在单位犯罪的语境下，企业领导人本应承担监管义务，而合规负责人需承担的合规制度建设义务并非企业犯罪危害结果的阻止义务，讨论二者的保证人义务并无意义。〔69〕以上两种观点发生冲突的原因是，对单位犯罪刑事责任根据的理解存在本质区别。依据本文主张的单位犯罪“决策机制责任论”，〔70〕合规计划不能替代对具体企业犯罪不法与责任的评价，其功能仅限于打开企业决策机制“黑箱”，厘清相关主体的权限分配，以明确企业运营中个人意志是否经企业决策机制认可而上升为企业意志，进而使个人犯罪行为上升为企业犯罪行为。

基于以上认识，企业领导人、合规负责人应承担的合规制度建设义务，的确不等于二者对企业犯罪应承担的保证人义务。在具体的企业犯罪刑事归责中，还需考察二者的保证人地位及具体监管义务。刑法通过构成要件创设了抽象的举止规范，其内容为一般性的构成要件结果阻止义务，其在具体行为情境下个别化为具体行为人的作为义务。具体而言，法规范认可的社会角色分工，即企业领导人与合规负责人属于企业意思形成或表示机关组成部分的身份，赋予二者对企业犯罪的保证人地位。在我国存在单位犯罪的语境下，明确二者的保证人地位，即认可二者事实上具备参与企业决策机制的资格。但是，保证人地位属于一般性命令规范的内容，只为二者赋予了一般性的构成要件结果阻止义务。除此以外，还需立足行为前视角，进一步明确依据二者身心能力与具体行为情境，采取避免具体构成要件中法益侵害危险实现的适格行为的义务；仅未履行合规制度建设义务，不会给二者带来刑事处罚风险。若二者在企业犯罪情境下未履行相应具体作为义务，则属于通过不作为参与企业决策机制，会促成其个人犯罪意志上升为单位意志，进而促成企业犯罪，需承担过失不纯正不作为犯的刑事责任。〔71〕因此，不能止步于证成企业领导人、合规负责人的保证人地位以确立其抽象的举止规范，还需明确二者具体应承担的作为（监管）义务。

在德国司法实践中，通过德国联邦最高法院作出的系列判决，企业合规负责人与企业领导人的保证人地位分别得到确立。〔72〕对于二者应承担的保证人义务应当具备业务关联性，理论界和实务界均无争议。转换到我国刑法语境，企业雇员犯罪行为的“业务关联性”，即为企业雇员的职权范围。传统主张主要以犯罪所得是否归于单位为依据，判断个人犯罪行为是否体现单位意志。本文认为，应以是否由领导（集体）直接决定，或是否符合公司议事决策章程、惯例与合规体系要求为标准，判断企业雇员的特定行为是否为企业决策机制所认可。对业务关联性判断标准，即“企业雇员实施的犯罪行为应与其职责相关，且体现其负责的业务类型”的内涵模糊的批判，在德国学界一直存在。以德国联邦最高法院 2018 年的判决为例，被告人是一家便利店店主，雇佣其兄弟为店员，其兄弟与另一店员一起利用该便利店客流量大、便于储藏、雇员少、窗户能阻挡视线等条件贩毒。判决认为，被告人对于具备以上条件的便利店能为贩毒提供便利条件有清晰的认识，但仍雇佣其兄弟担任店员，即应承担阻止其兄弟利用相关条件实施贩毒的保证人义务。针对此判决的批判意见认为，店员的贩毒行为并不是为了实现其工作目的，被告人与犯罪人的兄弟关系、雇佣关系，或为其提供场所与职权便利的行为，均未

〔69〕 参见李本灿：《合规官的保证人义务来源及其履行》，《法学》2020 年第 6 期，第 89 页以下；田宏杰：《刑事合规的反思》，《北京大学学报（哲学社会科学版）》2020 年第 2 期，第 127 页。

〔70〕 参见前引〔3〕，敬力嘉文，第 98 页以下。

〔71〕 参见敬力嘉：《网络不作为参与行为不法类型的重塑》，《政治与法律》2020 年第 11 期，第 42 页以下。

〔72〕 BGHSt 57，42；BGH，Beschl. v. 6. 2. 2018 – 5 StR 629/17.

升高其兄弟贩毒的风险，不能以此为依据认可被告人作为企业领导人的保证人地位。〔73〕

本文赞同以上批判意见。只有雇员从企业获得犯罪所需的特别工具、场所或数据等符合企业议事决策章程、惯例与合规体系要求，企业领导人才应当对雇员利用职务之便实施的不法行为承担保证人义务。在企业领导人具备保证人地位之后，合规负责人才能基于前者授权获得保证人地位。以此为前提，才能进一步在具体犯罪构成要件中判断二者应承担的监管义务。以企业成立侵犯公民个人信息罪为前提，以企业的个人信息保护合规计划为依据，针对企业所处行业、规模，及其实施的具体个人信息处理行为，可判断企业领导人、合规负责人应承担的具体监管义务。若二者未履行监管义务，则应作为主管人员或其他直接责任人承担单位犯罪的刑事责任。当企业领导人、合规负责人明确知悉其不履行监管义务的刑事处罚风险，二者基于成本收益的理性衡量，便可具备足够动力认真履行自己应当承担的监管义务。基于目的正当原则、区分原则、均衡原则与信赖原则的要求，以个人信息保护法第 54 条要求企业定期进行的个人信息保护合规审计为制度依托，企业领导人、合规负责人需严格审查个人信息保护合规计划的针对性，保障个人信息保护合规机制有效运行。至此，侵犯公民个人信息罪对于个人信息保护合规体系的底线保障功能及其实现路径得以全面厘清。

Abstract: Personal information protection compliance, as an enterprise management tool, faces a systemic risk of abuse. For this reason, when allocating the risk of the processing of personal information, the requirements of the principle of proportionality should be followed, and the freedom of individual citizens, enterprises and public authorities in processing personal information should be reasonably restricted, both of which should be taken as a legal basis of the compliance with personal information protection. Accordingly, when designing a compliance program for the protection of personal information, enterprises should follow the principles of legitimate purpose, distinction, balance and trust. When conducting a compliance audit of an enterprise's personal information protection, a three-step review method should be adopted, i. e., a progressive review of the general characteristics of the compliance program, the specific elements and their functions, and the specific acts of members of the enterprise. The bottom line of an enterprise's personal information protection compliance system is defined by the crime of infringing on citizens' personal information. By using the compliance of an enterprise's processing of personal information and the fulfillment of the supervisory obligations by the enterprise's leaders and compliance officers as the criteria to evaluate the wrongfulness of this crime, the bottom-line function of the crime can be effectively realized.

Key Words: personal information protection, enterprise compliance, compliance audit, the crime of infringing on citizens' personal information

〔73〕 参见 Dennis Bock, Zum Stand der Geschäftsherrenhaftung des Betriebsinhabers für betriebsbezogene Straftaten seiner Mitarbeiter (BGH, Beschl. V. 6. 2. 2018 – 5 StR 629/17 NStZ 2018, 648), 载前引〔34〕, Rotsch 编书, 第 1 页以下。