法商研究 Studies in Law and Business
Vol. 41 No. 2(2024)

个人信息保护企业合规规制的建构

谢 尧 雯*

摘 要:《中华人民共和国个人信息保护法》对企业内部管理程序提出了规范要求,并通过设定法律责任激励企业完善内部管理,形成了企业合规规制的基本框架。法律从界定企业行为的义务边界转向指引、激励企业完善内部管理,体现出超越"命令—控制"的规制理念,发展个人信息保护合作规制。个人信息保护企业合规规制需要在合规指引与合规激励两个方面加以完善。在完善合规指引方面,应确立"基于风险的规制"的合规理念,引导企业在具体场景中确定具体义务内容;同时,规范企业核心决策流程,提升企业责任能力。在完善合规激励方面,应构建个人信息保护事前合规激励机制,厘清行政责任中合规程序与危害后果的关系;同时,推动个人信息保护事后合规激励,通过合作式执法培育共同理性与合作信任。

关键词:个人信息保护 企业合规 合规指引 合规激励

一、问题的提出

企业合规是指通过法律规范企业内部管理程序,指引、激励企业完善内部具体管理,旨在提升企业实现法律实质目标的能力与效率。个人信息保护领域亦采用了这一规制工具。《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》)对企业内部管理程序提出了系列要求,如指定个人信息保护负责人、定期进行合规审计、开展个人信息保护影响评估等,并通过设定法律责任激励企业完善个人信息保护具体方案,形成了企业合规规制的基本框架。

合规规制表明法律介入了传统上属于企业自治的内控体系,相应制度设计须妥善平衡监管与自治的关系。一方面,法律介入旨在指引企业建立符合自身特征的内部管理机制,因此外部规范设计应当实现引导核心方向与留足自治空间的双重目标。另一方面,由于企业完善内部管理需要支出高昂的成本,因此法律体系有必要通过合理设置责任、创新执法手段等方式提供外部激励。从法律文本与执法现状分析,个人信息保护在这两个层面并未完成规范的制度设计。就外

* 中国政法大学法与经济学研究院助理教授
基金项目:国家社会科学基金资助项目(22CFX055)

部指引而言,由于《个人信息保护法》的条文规定过于抽象,因此企业到底如何运用内部管理措施实现公平、公正的个人信息处理,存在高度不确定性。就外部激励而言,法律仅规定企业违反内部管理义务将承担行政责任,但没有为企业执行抽象规定提供稳定预期和柔性执法关怀;在发生危害后果后,企业内部管理能否成为免除或减轻责任的依据,执法机关也未达成共识。

事实上,合规规制并非一仍旧贯,不同的规制工具彰显了不同的规制理念。在传统企业规制中,法律主要设置以生产方式为导向的"具体行为标准"和以生产结果为导向的"绩效标准"。美国量刑委员会于 1991 年发布的《联邦组织量刑指南》,将企业有效合规方案作为减轻刑罚的考量因素之一,并对有效合规方案的概念与核心构成进行了明确界定。这标志着监管部门开始介入传统上属于企业自治范畴的内部管理。[①] 此后,这种规制模式逐渐发展并拓展至环境保护、食品药品安全、职业健康、个人信息保护等多个领域。

从域外个人信息保护立法看,法律核心规制工具从具体行为标准转向合规管理标准。然而,对于这种转变的适当性以及如何完善合规规制,仍缺乏深入的理论分析。本文通过探寻个人信息保护企业合规规制的实践发展及法理基础,提出在设置指引与构建激励两个方面完善合规规制,从而尝试在个人信息保护领域建立企业合规规制的理论框架。

二、个人信息保护企业合规规制的确立

法律规制企业行为包括 3 种基本规制工具:一是"具体行为标准规制",强调以生产方式为导向,规定企业应当或禁止采用的技术标准或行为措施;二是"绩效标准规制",强调以生产结果为导向,规定企业须达到的结果目标;三是"合规规制",强调以企业决策过程为导向,规定企业内部管理体系,[②]又被称为"内部管理型规制"。[③]

个人信息保护立法始于 20 世纪 70 年代,是典型的规制法。在信息技术发展的不同阶段,法律亦采用不同的规制工具。在我国,《个人信息保护法》规范企业内部管理程序,确立了企业合规规制的基本框架,这与欧盟、新加坡等世界主要经济体的个人信息保护立法趋势也是相契合的。

(一)个人信息保护立法规制工具的演变

传统上,个人信息主要通过隐私权民事诉讼途径得到保护。[④] 自 20 世纪 70 年代以来,欧洲国家率先开始个人信息保护的事前监管立法。随着信息技术的发展,全球层面的个人信息保护立法进程不断推进。总体来说,个人信息保护立法旨在规范个人信息处理程序,但法律本身并不表达合法与违法处理行为的实质标准,而是通过设置决策程序,将合法与否的决策权赋予监管部

① See Kimberly D. Krawiec, Cosmetic Compliance and the Failure of Negotiated Governance, 81 Washington University Law Quarterly ,497－510(2003).

② 合规意味企业需要确保其行为符合监管要求,因此,合规与内部管理体系相联系,通常包含一套内部控制程序缓解违规风险。See Miriam H.Baer, Governing Corporate Compliance,50 Boston College Law Review,958(2009).

③ See Cary Coglianese & David Lazer, Management－Based Regulation: Prescribing Private Management to Achieve Public Goals, 37 Law and Society Review,693－696 (2003);国内学者的研究,参见谭冰霖:《论政府对企业的内部管理型规制》,《法学家》2019 年第 6 期。

④ See Jerry Kang, Information Privacy in Cyberspace Transactions,50 Stanford Law Review,1202(1998).

门、个人信息主体和个人信息处理者。[①] 因此，不论何种阶段或者基于回应何种技术的个人信息保护法律，其内容都包括两个核心要素：(1)设置实体规则对个人信息处理质量提出基本要求，以抽象绩效标准规制为主；[②](2)设置程序规则对各主体行使决策权进行规范，以具体行为标准规制与合规规制为主。[③]

总体来看，规范个人信息处理质量要求的绩效标准较为稳定，体现为较为抽象的结果要求，如确保信息处理公平和尊重个体权益等。关于信息处理是否合法的决策主导权经历了从监管部门到个人信息主体，再到信息处理者的转变。相应地，规制工具也从具体行为标准规制转向合规规制。[④] 这种转变大致呈现为以下 3 个阶段。

第一阶段：监管部门享有决策主导权。在 20 世纪 70 年代初期，大型主机的发展带来了中心化与规模化的信息处理模式。瑞典、荷兰等欧洲国家通过制定法律来保护公民隐私权益。这一阶段法律内容的核心特征是，监管部门通过行政许可机制，决定信息处理者是否可以开展以及如何开展信息处理。[⑤]

第二阶段：个人信息主体享有决策主导权。在 20 世纪 70 年代中后期，随着通用计算机的普及，信息处理逐渐去中心化。这一阶段法律内容的核心特征是，个人信息主体拥有对个人信息的绝对控制权，由他们决定信息处理者是否可以开展以及如何开展信息处理。[⑥]

第三阶段：个人信息处理者享有决策主导权。随着数字技术的发展，信息处理程序越来越复杂。这一阶段法律内容的核心特征是，法律规定愈发抽象，依赖个人信息处理者在具体场景中确定如何进行信息处理，并设置大量条文规范企业的内部管理程序。其典型代表就是欧盟委员会于 2018 年施行的《欧盟一般数据保护条例》(以下简称《一般数据保护条例》)。

前两个阶段的义务规范以具体行为标准为主要表现形式，即法律明确规定处理者向监管部门申报许可的具体要求、为个体行使控制权提供具体保障。个人信息处理者以“勾选框”的方式履行义务。[⑦] 第三阶段的义务规范以内部管理型标准为主要表现形式，即法律规定内部管理的一般要求，引导、激励企业结合自身情况制定具体的个人信息处理方案。

(二)个人信息保护企业合规规制的基本框架

《个人信息保护法》基本符合个人信息保护立法第三阶段的特征，即设定大量针对企业内部

---

① See Claudia Quelle, Privacy, Proceduralism and Self－Regulation in Data Protection Law, 1 Teoria e Critica della Regolazione Sociale, 93－94(2017).

② 绩效标准包括抽象目标导向与具体结果要求两种形式。See Cary Coglianese, The Limits of Performance－Based Regulation, 50 University of Michigan Journal of Law Reform, 537－538(2017).

③ See Herbert Burkert, Data－Protection Legislation and the Modernization of Public Administration, 62 International Review of Administrative Science, 558(1996).

④ See Claudia Quelle, Privacy, Proceduralism and Self－Regulation in Data Protection Law, 1 Teoria e Critica della Regolazione Sociale, 96－101(2017).

⑤ See Gloria G. Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer, 2014, pp.59－65.

⑥ See Viktor Mayer－Schönberger, Generational Development of Data Protection in Europe, in Philip E. Agre & Marc Rotenberg eds., Technology and Privacy: The New Landscape, MIT Press, 1997, pp.226－230.

⑦ See Milda Macenaite, The “Riskification” of European Data Protection Law Through a Two－Fold Shift, 8 European Journal of Risk Regulation, 515(2017).

管理的条款,构建了合规规制的框架。

一般来说,合规规制框架包括“基本程序”与“激励机制”两个部分。一是监管部门制定程序规则,对企业内部管理提出基本要求。同时,内部管理型规制往往体现为一种目标导向的程序机制,即与具体行为标准规制、绩效标准规制相结合,促进后两种规制要求的实现。① 当内部管理型规制与具体行为标准规制相结合时,其通常要求企业建立内部管控体系,以此确保雇员行为符合具体规定要求。二是企业制定、实施内部管理方案需要投入高昂成本,因此,责任惩戒、合规不起诉、合规不处罚等执法措施对于激励企业完善内部管理至关重要。

就此而言,我国个人信息保护企业合规规制框架体现为:(1)《个人信息保护法》第 5 章对企业内部管理提出了要求,包括制定内部管理制度和操作规程、指定个人信息保护负责人、开展个人信息保护影响评估等;第 1 章、第 2 章、第 4 章对企业个人信息处理提出了较为抽象的结果要求,包括处理个人信息应当保证个人信息的质量、保障个人信息主体的权利等。这表明,《个人信息保护法》采取了内部管理型规制与抽象绩效标准规制相结合的形式。(2)《个人信息保护法》第 7 章对企业违背内部管理义务设置了法律责任,督促企业完善内部管理。

三、个人信息保护企业合规规制的目标

企业决策与个人决策存在显著差异,其特征体现为企业内部不同个体的共同作用,以及企业整体文化环境影响个体思维。② 因此,法律规范企业内部管理有助于打开决策黑箱,促使企业将外部监管目标嵌入内部运行体系。但是,法律介入企业自治将耗费大量执法资源,相关制度设计需要平衡好监管与自治的关系。

在个人信息保护领域,法律从界定企业行为的义务边界向指引、激励企业完善内部管理,体现了超越“命令—控制”的规制理念,发展个人信息保护合作规制,实现对企业自我规制的再规制。审视规制理念转变是否理性回应了信息技术发展、合规规制在新规制理念下承担了何种职能,成为寻求法律监管与企业自治平衡的前提。

(一)个人信息保护机构问责理念的建立

个人信息保护最初承袭于隐私保护,但随着数字技术的不断发展,二者呈现出不一样的价值基础与规制路径。隐私保护建立在“个体—社会”二元划分的社会结构预设中,隐私权是个人自主调节私人与公共界限的工具。在私人领域,个人拥有隐藏或分享信息的决策权,以控制外界访问;而一旦暴露于公共空间,则意味着个人被迫放弃了对于隐私的主张。③ 因此,隐私保护主要依托个人自主控制。

在 20 世纪 70 年代初期,法律通过设置行政许可来规制大型主机的个人信息处理。但随着个人信息处理的去中心化发展,行政许可制度被迅速淘汰。由于信息隐私一直是隐私保护的重

① See Sharon Gilad, It Runs in the Family: Meta-Regulation and Its Siblings, 4 Regulation & Governance, 489-491 (2010).

② See Edward L. Rubin, Images of Organizations and Consequences of Regulation, 6 Theoretical Inquiries in Law,352-366(2005).

③ 参见余成峰:《数字时代隐私权的社会理论重构》,《中国法学》2023 年第 2 期。

要内容，个人控制理念对个人信息保护立法产生了深远的影响。长期以来，个人信息保护立法的规则设计围绕“帮助个人理解和控制与他们有关的信息”展开。数字技术发展对个人控制理念以及以此为基础的具体行为标准规制，带来了以下两大挑战，促使个人信息保护树立机构问责理念。

1.个人信息与非个人信息边界逐渐模糊

数据是记录、分析和重组内容的载体，而信息则是附着在数据之上具有一定意义的内容。[①] 其中，“个人信息”的核心意义为“可识别性”，即单个信息或与其他信息结合可以识别到个人特征。早期，数据承载的内容有限，数据处理亦只限于某些特定行业与具体环节。并且，技术赋予信息“可识别”意义的方式并不复杂，个人信息与非个人信息的区分标准较为明确且客观。因此，长期以来，法律适用采取“个人信息/非个人信息”二元划分的“全有全无”路径，即某些信息要么受个人信息保护法的保护，要么完全不受法律保护。[②]

数字技术的发展使得大量信息得以转换为机器可读的形式，各行各业的活动都开始以数据处理为基础。在高度互联的智能化环境中，人工智能以自我学习、自我管理来建构数据之间的关联、挖掘数据内部的可识别意义，使得数据所承载的所有信息都可能在主观预期影响或者客观结果影响层面与个人相关联。由此，个人信息与非个人信息的边界逐渐模糊。

从保护个体权益角度来看，由于所有信息都存在识别或关联个人的可能性，个人信息与非个人信息的区别失去了实质意义，因此个人信息保护法律有必要摒弃区分个人信息与非个人信息的“全有全无”适用模式，其需要通过广泛适用来承担数字空间基本法的职能。这也意味着，个人信息保护法律规则将影响极其广泛的社会活动，法律应当平衡多元利益，而不是对彰显隐私利益的个人控制权提供绝对保护，以此解决更多社会问题。[③]

2.群体隐私隐患日渐凸显

数字技术发展正将关注焦点从传统的个体信息转向群组信息。数字画像通过群体行为特征知识构建各类群组标签，个体信息只是作为数据点被化约性地纳入其中，由此产生群体隐私被侵犯的隐患。[④] 在保护群体隐私的语境下，个人控制信息的决定很可能对社会群组产生负外部影响。并且，即使个体具备充分理性，也只能控制自己的信息，无法影响大数据算法所运行的信息环境，也无法预防群体隐私被侵犯的风险。

以上两大挑战促使个人信息保护理念与隐私保护理念逐渐产生区别。个人信息处理程序是否开展与如何开展，无法通过界定清晰规则的方式交由监管部门或信息主体决定，而是越来越依赖个人信息处理者在具体场景中的判断。这促使个人信息保护理念从个人控制转向机构问责。

（二）机构问责理念下企业合规规制的意涵

法律需要为个人信息处理者提供宽泛的裁量空间，这依赖规范形式的原则化转变。法律规

① 参见时建中：《数据概念的解构与数据法律制度的构建——兼论数据法学的学科内涵与体系》，《中外法学》2023年第1期。

② See Nadezhda Purtova, The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law, 10 Law, Innovation and Technology, 56－59(2018).

③ 参见赵鹏：《个人数据保护的合作治理模式研究》，《人民论坛·学术前沿》2023年第6期。

④ See Brent Mittelstadt, From Individual to Group Privacy in Big Data Analytics, 30 Philosophy & Technology, 477－481(2017).

范包括“规则”与“原则”两种基本形式。规则对行为模式和后果进行具体和详尽的规定,是确定性命令;原则体现为抽象价值与行为方向的指引,是最佳化命令。① 在规制实践中,大多数规范内容并不体现为纯粹规则或纯粹原则,而是呈现不同明确程度的行为指引谱系。根据规制的明确性程度,法律规制可分为原则化规制与规则化规制。原则化规制是指,在适用法律时判断什么是法律允许和禁止的行为;规则化规制是指,法律事先规定什么是法律允许和禁止的行为。②

欧盟个人信息保护法律的发展,体现了规则化规制向原则化规制的转变。相较于《关于个人数据处理及其自由流动的个人保护第 95/46/EC 号指令》(以下简称《1995 年指令》),《一般数据保护条例》原则化规制发展主要体现在两个方面:一是个人控制权规则的例外适用情形增多,导致规则适用标准愈发模糊,权利呈现明显的价值属性而非规范属性;③二是《1995 年指令》要求成员国颁发确定的规则来规制数据处理,而《一般数据保护条例》直接规制公民个体,并要求信息处理者在具体场景中为原则化规范填充具体内容。

原则化规制表明个人信息处理者在适用法律的过程中解释了法律,即在具体场景中将抽象规定转化为具体的个人信息处理方案。这意味着,个人信息处理者承担了重要的公共规制职能。④ 为约束信息处理者的权力,中国、欧盟、新加坡等国家和地区在个人信息保护法律中引入了“问责原则”,确立了机构问责理念。

在语言结构上,“问责”由“解释”和“能力”构成,意指解释的能力。问责原则要求,行为者向外部监督者解释其行为的方式与理由,旨在通过外部审查内部决策体系的方式,实现规范权力主体行为的目的。⑤《个人信息保护法》第 9 条要求个人信息处理者对个人信息处理活动负责,并采取必要措施保障个人信息安全,这充分体现了责任原则。

在问责原则的落实中,企业内部管理发挥核心作用。它不仅负责将抽象的法律要求转化为具体的个人信息保护方案,而且决定企业如何实现法律目标。⑥ 因此,个人信息保护法律介入企业内部管理,主要目的在于构建“政府—企业”的合作规制结构,确保企业行为遵循规范的决策流程和科学的决策逻辑,从而增强企业的责任能力。

四、完善个人信息保护企业合规的指引

完善企业合规规制的首要任务是法律如何设置程序指引,既规范企业内部管理,又尊重企业

① 参见[德]罗伯特·阿列克西:《法:作为理性的制度化》,雷磊编译,中国法制出版社 2012 年版,第 149 页。

② See Louis Kaplow, Rules Versus Standards: An Economic Analysis,42 Duke Law Journal,560(1992).

③ 面对复杂的规制对象,立法设置的大量例外情形增加了规则适用的不确定性,呈现规制原则化特征。See John Braithwaite, Rules and Principles: A Theory of Legal Certainty, 27 Australian Journal of Legal Philosophy,60—75(2002).

④ See Kenneth A. Bamberger, Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State,56 Duke Law Journal,386—392 (2006).

⑤ See Mark Bovens, Analysing and Assessing Accountability: A Conceptual Framework,13 European Law Journal,450—453(2007).

⑥ See Joseph Alhadeff,Brendan V. Alsenoy & Jos Dumortier,The Accountability Principle in Data Protection Regulation:Origin,Development and Future Directions, in Daniel Guagnin et al. eds., Managing Privacy Through Accountability, Springer,2012,pp.65—66.

自治。原因在于,内部管理型规制旨在弥补自上而下“命令—控制”模式与自下而上自我规制模式的不足,通过构建一个介于两者之间的“元规制”模式,促使规制对象针对公共问题作出自我规制式的内部回应。《个人信息保护法》确立的规制理念与规制工具,是对技术发展的理性回应。但现阶段,企业如何通过内部管理程序实现公平与公正的个人信息处理,仍然非常模糊。一方面,内部管理程序是具体化抽象法律要求的媒介,但个人信息处理者在具体场景中如何权衡不同利益、如何确定具体义务内容,仍缺乏基本的合规理念指引。另一方面,法律文本对内部管理程序的规定过于抽象,难以实现提升企业问责能力的目标。为此,在构建《个人信息保护法》的法律配套实施机制中,尤其需要关注基本合规理念的确定与内部管理结构体系的完善。

(一)确定“基于风险的规制”的合规理念

企业在具体场景中以何种方式适用原则性法律规定,存在不确定性。为了降低这种不确定性,欧盟在个人信息保护中引入“基于风险的规制”的合规理念,引导企业在具体场景中根据风险大小制定具体方案,值得借鉴。① “基于风险的规制”作为一种提升决策能力的工具,强调通过测量损害发生的可能性与严重性来配置规制资源,从而将不确定性转化为可以认知与控制的对象。以此作为企业合规理念,需要在以下两个方面进行制度设计。

1.根据风险大小确定个人信息处理者的具体义务内容

“基于风险的规制”的合规理念为个人信息处理者适用法律提供了一个程序框架,而不是确切的义务内容。在这一程序框架下,个人信息处理者根据信息处理对个体权益影响与保障措施成本等因素,确定是否开展以及如何开展信息处理活动,从而在具体场景中落实保障个人信息处理质量等法律抽象结果要求,以及采取安全保障措施等抽象程序要求。因此,“基于风险的规制”的合规是一个由“活动”“附加义务”和“义务豁免”构成的合规体系。在这一体系下,信息处理活动分为高风险、中风险和低风险等不同类别,每类活动对应不同的附加义务,一些义务在特定条件下可以得到豁免。信息处理者必须证明其根据不同风险类别采取恰当的技术和组织措施。②

2.“基于风险的规制”与“基于权利的规制”之协调

在个人控制权占主导地位的传统个人信息保护法律中,信息处理者有义务对个人信息主体的同意权、访问权等各项控制权能给予平等和绝对的保护,这与“基于风险的规制”强调差异化保护存在一定冲突。③ 为了调和这一冲突,欧盟第 29 工作组于 2014 年倡导引入“基于风险的规制”合规理念时声明,“基于风险的规制”仅仅是“基于权利的规制”的补充,个人信息处理者仍然需要对个人信息主体权利给予平等的保护,只有权利体系外的义务才能根据风险进行伸缩与调节。④

---

① See Claudia Quelle, Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-Based Approach, 9 European Journal of Risk Regulation, 504-508(2018).

② 参见刘泽刚:《大数据隐私权的不确定性及其应对机制》,《浙江学刊》2020 年第 6 期。

③ “基于风险的规制”能否进入规制领域,很大程度上取决于特定监管区域对公民平等受保护权理念的重视程度。See Henry Rothstein, Olivier Borraz & Michael Huber, Risk and the Limits of Governance: Exploring Varied Patterns of Risk-Based Governance Across Europe, 7 Regulation & Governance, 229-230(2013).

④ See Article 29 Data Protection Working Party, Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf, 2023-04-10.

随着个人信息概念的逐步扩张,法律需要平衡的权益越来越多,权利规范亦转向原则化形式。由于原则的适用方式是权衡,因此“基于风险的规制”的方法可以为原则性权利提供切实可行的保障机制。但是,在将“基于风险的规制”适用至原则性权利保护时,规制者需要通过更为精细的制度设计,协调平等保护理念之间与差异化保护理念存在的价值冲突。① 一方面,应当将风险的大小作为保护个人信息主体权利的前提条件。因此,须摒弃划分个人信息与非个人信息的传统路径,转而在普遍适用《个人信息保护法》的基础上,根据特定信息在具体场景中被识别的概率以及不当使用或泄露带来的损害来决定是否以及如何保护个人信息主体控制权。另一方面,个人对信息的适度控制彰显个体自我决定价值,对于个体在数字空间中发展独立数字人格具有重要的道德意义。这表明,在涉及人的尊严等具有强烈伦理价值的重要权利领域,应当谨慎引入功利性计算方法。为此,规制者需要探究个人信息控制权核心的道德边界,在这个边界以内,权利行使依个体意愿而无关风险水平。②

(二)完善企业内部管理结构

企业由多个雇员与部门组成,其行为受宏观组织决策与微观个体决策的影响。因此,如果法律希望通过介入内部管理的方式提升企业责任能力,就要在企业决策可能背离法律实质要求的关键节点创设有效的反思结构进行控制。根据组织决策基本原理,以下两类决策影响可能导致企业行为偏离法律实质性要求,包括:(1)在宏观组织决策方面,决策惯性导致企业难以适应环境变化。标准化生产流程塑造了稳定、可预期的决策环境,提高了效率,但也可能导致企业忽视复杂信息,不够关注过程变化,并依赖传统方法处理新问题。当前个人信息处理环境变化频繁,数据规模扩大、算法能力提升和技术攻击等诸多变化会不断产生新的风险。企业若过度依赖稳定决策逻辑,则将缺失反思和适应新风险的能力,难以调整内部管理措施来应对新问题和挑战。(2)在微观个体决策方面,部门分工削弱了企业控制成员违法行为的能力。企业由单个个体与部门结合组成,雇员或部门行为是企业对外施加影响的媒介。但是,如果雇员或部门为了自身利益违背法律要求或者错误理解法律要求,就会导致企业行为偏离法律目标,而个人或部门工作的细化又会进一步增加违规的概率。个人信息保护牵涉到企业运营的各个层面:直接面向客户的业务运营层需要在个人信息收集与数据产品应用中保护个人信息;设计产品的技术支撑人员需要将个人信息保护要求嵌入产品设计中;③负责管理的后台服务人员需要确保数据存储、流通与利用符合个人信息保护的要求。因此,分工与细化带来的信息不对称、部门隐私伦理专业素能缺失、违规行为隐匿化等问题,将严重减损企业保护个人信息的能力。

综上,法律通过规范内部管理程序提升企业责任能力,需要在宏观组织决策层面提升企业对外部风险的学习与适应能力,在微观个体决策层面提升成员执行企业个人信息保护方案的能力。

1.通过完善影响评估制度优化企业个人信息保护方案

---

① See Claudia Quelle, The Risk Revolution in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too, in Ronald Leenes et al. eds., Data Protection and Privacy: The Age of Intelligent Machines, Hart Publishing, 2017, pp.33－60.

② 参见赵鹏:《“基于风险”的个人信息保护?》,《法学评论》2023 年第 4 期。

③ 有学者通过调查发现,大部分美国科技企业产品设计部门缺乏隐私伦理专家,缺乏将个人信息保护理念嵌入产品设计的专业能力。See Ari E. Waldman, Designing Without Privacy, 55 Houston Law Review, 675－678 (2018).

个人信息保护影响评估要求企业通过分析信息处理引发的影响来决定是否开展与如何开展个人信息处理程序，它是企业将抽象法律要求转化为具体个人信息保护方案的核心程序。[①] 根据《个人信息保护法》第55条的规定，个人信息处理者仅在处理程序开始前与特定情形下才有义务开展个人信息保护影响评估。由于相关程序相对静态与封闭，因此容易产生企业决策的路径依赖，从而导致企业难以回应新风险。从提升企业学习与适应变化的风险管理能力的角度看，至少可以从以下两个方面进行制度完善：

第一、将个人信息保护影响评估拓展至个人信息处理的整个生命周期。首先，应重视“记录义务”对企业提升风险管理能力的重要性。企业组织学研究表明，要求企业详细记录决策过程，且允许监管部门查阅这些记录，实质是要求企业时刻准备向监管部门解释其决策逻辑，能够助推企业打破惯性思维，促使其考虑更多相关因素。[②] 因此，要求企业详细记录信息处理的规模、目的、合法性基础、技术与组织保障措施等，并允许监管部门进行查阅，有助于企业更好地评估和管理风险，并加强与监管部门的合作与沟通。由此看来，记录义务在一定程度上既发挥了影响评估的制度功能，又没有为企业施加过重负担。《一般数据保护条例》将影响评估义务局限于特定高风险场景，但在第30条明确规定了记录义务，这实质上构建了一个层次化的影响评估体系。其次，对于达到一定规模的处理系统、自动化决策系统和涉及敏感信息处理系统等高风险信息处理系统，有必要对其设定定期评估义务。根据欧盟第29工作小组发布的指引，企业需要定期审查影响评估的实效性。[③] 近年来，新加坡个人信息保护执法机构不断加强对企业内部合规计划的审查，企业未定期测试、评估其技术保护措施的有效性，这些都构成行政处罚的重要事由。[④]

第二、适度开放个人信息保护影响评估程序。《个人信息保护法》并未要求企业纳入利益相关人参与评估、公开评估报告，在一定程度上平衡了企业的商业利益与社会责任。在信息技术及其支撑的商业模式对社会产生越来越重要影响的情况下，增强企业社会责任最为典型的两种开放程序方式——吸纳利益相关人意见和公布企业社会责任报告——值得个人信息保护法律体系的重视。(1)将利益相关人纳入影响评估程序。不同于传统技术对环境与安全造成的物理性影响，数字技术对社会的影响更多是关乎生活方式、道德理念的价值性影响。在伦理多元化的社会中，将利益相关人纳入影响评估程序，有助于提升制度的规范性与科学性。在规范性层面，公众参与能够促进科技发展的民主化进程。当公众参与到具有重大变革潜力类信息科技的影响评估程序、表达“我想要何种生活方式”的价值选择时，科技发展方向就不再是少数人的独断，而是社会整体的决策。[⑤] 在科学性层面，公众参与推动企业作出更全面与负责任的评估结论。个人信

① See Reuben Binns, Data Protection Impact Assessments: A Meta－Regulatory Approach, 7 International Data Privacy Law,22－23(2017).

② See Philip E. Tetlock, Accountability: The Neglected Social Context of Judgment and Choice,7 Research in Organizational Behavior,314－321(1985).

③ See Morgot E. Kaminski & Gianclaudio Malgieri, Algorithmic Impact Assessments Under the GDPR: Producing Multi－Layered Explanations, 11 International Data Privacy Law,130(2021).

④ See Steve Tan & Justin Lee, Being Accountable in Transforming Your Business for Data Innovation—Learning Points from the Personal Data Protection Commission's Enforcement Decisions in 2019, in Yeong Zee Kin ed., Personal Data Protection Digest, Academy Publishing,2020, pp.28－32.

⑤ 参见赵鹏、谢尧雯：《科技治理的伦理之维及其法治化路径》，《学术月刊》2022年第8期。

息保护影响评估需要权衡 3 个因素:信息处理的正、负面影响及缓解负面影响的成本。其中,负面影响多体现为难以量化的情感与认知影响,包括破坏声誉、削弱谈判能力、因缺失对个人信息的控制而产生的恐惧与失望等。因此,受影响利益群体参与评估、向企业提供直接与具体的体验和感受,对于提升企业的学习能力至关重要。(2)适度公开个人信息保护影响评估报告。信息披露作为市场监管工具,旨在增强市场资源配置效率和提升投资者与消费者的理性决策能力。因此,市场监管类法律要求企业向市场披露的信息,主要涉及对消费者和投资者决策有重大影响的信息。在当前市场环境中,个人信息保护通常不是影响投资者决策的重要因素,这意味着评估报告仅属于上市企业自愿披露的信息。① 但是,与"记录"功能类似,企业在意识到决策结果将受到外界评论或审查时,将会更加倾向于以审慎与负责的态度开展个人信息保护影响评估。② 再者,《个人信息保护法》并未规定企业如何落实风险管控措施,这很有可能导致评估沦为形式化的合规流程。适度的信息披露可以发挥市场监督功能,督促企业逐步落实并完善风险缓解措施。根据《个人信息保护法》第 58 条的规定,超级平台需要定期公布个人信息保护社会责任报告。但是,法律关于超级平台的定义并不明晰,导致信息披露功能并未充分发挥。未来应探索公开个人信息保护影响评估报告的具体路径。

2.通过完善组织建制塑造企业合规文化

企业组织文化通过影响成员的行为逻辑潜移默化地将企业战略目标与行为标准嵌入其日常行为模式。③ 因此,在微观层面提升企业问责能力的关键在于,塑造个人信息保护合规文化,促使个人信息保护理念与标准被贯彻到前台客户运营、中台产品设计、后台数据管理的全过程。

在食品安全、环境保护、消防安全等规制实践中,法律通过设置内部管理专员形成专门组织建制的方式,帮助企业营造合规文化。④《个人信息保护法》第 52 条设置"个人信息保护负责人"作为企业内部管理专员来监督企业的个人信息处理活动。这表明,立法者已经意识到专门组织建制对于提升企业合规水平的重要性,但既有规定过于简略,需要在确定核心职责与完善履职保障两个方面进行制度完善:(1)确定"个人信息保护负责人"的核心职责。个人信息保护合规文化旨在激励成员自主、积极遵守企业个人信息保护理念与管理计划。因此,"个人信息保护负责人"需要确保企业成员了解企业的个人信息保护方案、具备专业素养,并遵从企业方案。就此而言,"个人信息保护负责人"的核心职责应当包括:交流、监督与激励。就交流而言,"个人信息保护负责人"可以通过知识培训与日常交流、咨询建议等方式,帮助成员了解其业务涉及的个人信息保护理念与行为准则。就监督而言,"个人信息保护负责人"应当定期审查企业内部各个运营环节是否符合个人信息保护管理规范、设置举报热线接受违规行为举报,在必要时对相关处理程序提出建议与指引。就激励而言,个人信息保护专员有必要督促企业就信息处理行为建立公平的惩

① 关于上市企业信息披露范围的论述,参见徐文鸣、刘圣琦:《新〈证券法〉视域下信息披露"重大性"标准研究》,《证券市场导报》2020 年第 9 期。

② 关于信息披露对企业决策的影响,See Kenneth A. Bamberger, Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State,56 Duke Law Journal,451(2006).

③ See David Hess, Ethical Infrastructure and Evidence－Based Corporate Compliance and Ethics Programs: Policy Implications from the Empirical Evidence, 12 New York University Journal of Law and Business,347－351 (2016).

④ 参见谭冰霖:《论政府对企业的内部管理型规制》,《法学家》2019 年第 6 期。

奖机制，以此激励成员积极践行符合伦理标准的信息处理准则。(2)完善“个人信息保护负责人”的履职保障。“个人信息保护负责人”核心职责的顺利履行，需要专业性、独立性与稳定性的支撑，外部监管有必要为其提供履职保障。其一，“个人信息保护负责人”必须具备必要的知识与技能，并符合相应的专业素养标准。为保障专业性，法律可以通过设立职业资格许可等方式进行规范和监管。其二，“个人信息保护负责人”享有直接向高层管理人报告的权力或由高层管理人担任，且可以直接访问企业成员个人信息处理程序。同时，为避免利益冲突，“个人信息保护负责人”不得进行个人信息处理，且不得接受处理者指示。其三，“个人信息保护负责人”与企业存在监督与被监督关系，法律应当对“个人信息保护负责人”的执业环境提供消极防御，如不得因为履行职务而遭受歧视与解雇。

五、个人信息保护企业合规激励机制的构建

基于科学的企业合规指引，接下来的问题是，监管部门如何设置有效的外部激励，推动企业结合具体实践设置有效的内部管理计划。这是因为，企业完善内部合规体系需要投入大量成本，如果没有外部激励，企业将缺乏发展和实施合规计划的动力。

在实践中，政府监管主要通过4种方式激励企业完善内部管理。一是法律直接为企业设定内部管理义务，并通过责任惩戒来威慑企业履行义务。二是在企业发生违法行为后，将企业是否执行有效的内部合规方案作为判断企业是否尽到注意义务的重要标准，从而认定企业是否违法以及如何承担责任。三是在执法策略方面，监管部门在执法中与企业达成关于完善内部合规结构的和解协议，包括不起诉协议、暂缓起诉协议、行政和解协议等。如果企业完善内部合规结构有助于预防未来风险，那么可以减轻或免除其责任。四是将企业内部管理结构作为行政许可的条件。

《个人信息保护法》主要采取第一种激励方式，即企业有义务完善内部管理，违背相关义务将承担行政责任。但这种激励方式存在诸多问题。其一，企业通过内部管理程序，将法律的抽象目标转化为具体结果。如果责任设置未能细致权衡程序与结果的关系，那么将导致法律承载的规制价值无法实现。其二，法律为企业设定的义务内容以原则性规定为主，导致企业行为缺乏明确指引。设置过于宽泛或严苛的法律责任，会减损市场对法治的稳定预期与监管信任。为此，在完善《个人信息保护法》法律配套实施机制时，需要补充建立事前合规激励与事后合规激励机制。

(一)构建个人信息保护的事前合规激励机制

事前合规激励指，在发生危害后果后，企业事先建立的内部合规体系可以成为免除或减轻法律责任的依据。[①] 这一机制的核心法理基础在于，企业是具有独立意志的行动主体，而内部合规管理是判断企业是否存在主观过错的重要参考。[②] 在我国刑事司法实践中，事前合规激励主要体现为合规无罪抗辩。企业若能够证明其对员工进行了充分的合规管理，则无须为员工的犯罪行为承担刑事责任。[③] 在个人信息保护的刑事司法领域，我国初步建立了事前合规激励制度。

① 参见熊樟林：《企业行政合规论纲》，《法制与社会发展》2023年第1期。

② 参见谭冰霖：《单位行政违法双罚制的规范建构》，《法学》2020年第8期。

③ 参见陈瑞华：《企业合规制度的三个维度》，《比较法研究》2019年第3期。

例如,在“雀巢公司员工非法获取公民个人信息案”①中,甘肃省 兰州市中级人民法院认为,雀巢公司的内部管理完备,无须为涉案员工非法获取公民个人信息的个人行为承担刑事责任。

个人信息保护以行政规制为核心,企业主要承担行政责任,②但现阶段事前行政合规激励制度还比较薄弱。由于个人信息保护中的行政责任与刑事责任存在显著差异,因此事前行政合规激励的考量重点应与刑事合规激励有所区别。③ 这体现在以下两个方面:一是合规程序的作用不同。在刑事法上,由于侵犯公民个人信息类犯罪的构成要件非常清晰,即企业通过内部合规监督成员遵守外部规则要求,因此在危害后果发生后,内部合规起着切割企业责任与成员责任的作用。在行政法上,法律对个人信息处理的质量提出抽象结果要求,并依赖内部合规程序将其转化为具体结果。因此,在危害后果发生后,内部合规成为判断特定损害可非难性的标准。二是合规方案的内容存在差异。在刑事法上,合规方案主要关注程序,如发布手册、进行员工培训等,从而将外部规则嵌入企业内部体系。在行政法上,合规方案更为复杂且专业,既包括实体内容,如企业根据法律抽象要求制定的具体个人信息保护规则,也包括将这些规则传达给员工的程序内容。就此而言,构建个人信息保护事前行政合规激励机制,须明确合规程序与危害后果之间的关系,并完善有效合规方案认定体系。具体而言:

1.明确合规程序与危害后果的归责关系

《个人信息保护法》通过规范内部决策程序提升企业风险预防能力,此种事前风险预防有别于基于危害结果开展惩戒的事后监管。在风险预防理念下,信息处理后果与企业决策相关,企业责任与企业重视风险的程度以及是否采取恰当措施直接相关。④ 因此,个人信息保护领域的归责原则是过错责任。内部合规是否完备成为判断企业是否尽到注意义务的核心标准。

根据《中华人民共和国行政处罚法》(以下简称《行政处罚法》)第 33 条第 2 款的规定,当事人有证据足以证明没有主观过错的,不予行政处罚。这表明,行政处罚从客观归责转向了过错责任,有责性成为与该当性、违法性并存的应受行政处罚行为的成立要件。此外,主观过错在行政处罚中不仅影响“定罚”,也影响“量罚”。这是因为,与侵权责任所强调的恢复正义不同,行政处罚的直接目的是惩戒与制裁。行政处罚的伦理性因素表明,究竟需要给予违法行为主体多大的非难与违法行为的情节具有一定的关联,主观恶性不可避免地会成为一个影响要素。⑤因此,在发生数据泄露、侵犯个人信息主体权利等危害后果后,内部合规程序的完备程度实质上构成判断企业直接故意、间接故意、重大过失、一般过失、无过错等主观过错状态的标准,成为减免处罚的重要事由。

2.完善有效合规方案的认定体系

在金融、食品药品等领域,我国监管部门已经发布大量指南来明晰合规标准,形成由政府主

① 参见甘肃省兰州市中级人民法院(2017)甘 01 刑终 89 号刑事裁定书。

② 参见孔祥稳:《论个人信息保护的行政规制路径》,《行政法学研究》2022 年第 1 期。

③ 目前,对于《中华人民共和国个人信息保护法》中个人信息主体权利保护采取何种保护方式的问题,学界尚存争议。笔者赞同王锡锌教授的观点,即应当以行政监管为中心对个人信息权利束进行保障。因此,本文论述的合规激励以行政合规激励为主。参见王锡锌:《重思个人信息权利束的保障机制:行政监管还是民事诉讼》,《法学研究》2022 年第 5 期。

④ 参见[德]尼克拉斯·卢曼:《风险社会学》,孙一洲译,广西人民出版社 2020 年版,第 111~112 页。

⑤ 参见熊樟林:《〈行政处罚法〉主观过错条款适用展开》,《中国法学》2023 年第 2 期。

导的有效合规方案认定体系。但是,《个人信息保护法》是个人信息保护领域的一般性法律,不同行业的数据处理需要根据实际情况确立不同的利益权衡标准。并且,数字技术发展加快了商业模式的更新迭代,这导致监管部门在判断有效合规方面存在信息赤字与专业短板。为弥补政府监管的局限性,一个重要的趋势是推动各行业形成个人信息保护行为准则,发展由市场主导的有效合规方案认定体系。

在制定和执行行业行为准则方面,各行业面临集体行动困境难题。因此,为在行业层面构建系统化与组织化的社会自我规制体系,政府监管层面的激励与规范至关重要。一方面,行业层面普遍缺乏制定和执行行为准则的动力。政府监管可以通过完善罚则、引入第三方监督和认证等激励手段,提升企业遵从的积极性。① 另一方面,行业行为准则通常由利益团体主导制定,易沦为大企业排斥竞争的工具,也可能因为缺乏商谈而导致其无法反映产业实践和需求。② 故政府监管有必要规范行业行为准则制定,确保程序的公正性与广泛代表性。

欧盟高度重视将一般性规定转化为具体行业的数据保护行为准则,并在《一般数据保护条例》第 40 条、第 41 条和第 83 条中设置了激励和规范机制,为我们提供了有价值的参考。在激励机制方面,欧盟鼓励成员国数据监管部门设置第三方专业机构监督企业执行行业准则,并赋予该机构对违规企业采取剥夺或暂停其行为准则适用资格的惩罚权力。此外,企业执行行业行为准则不仅是获取市场信任的方式,也是证明其行为合规的重要依据,有助于获得处罚减免。在规范机制方面,只有获得成员国数据监管部门批准的行为准则,才具备合规证明效力。监管部门批准的关键条件是,行业准则的制定过程必须遵循开放和公平的原则。③

(二)构建个人信息保护事后的合规激励机制

事后合规激励指,企业涉嫌违法行为发生之后,监管部门对企业开展内部重整,如果内部重整达到有效合规标准,那么可以对企业减免处罚。④ 在刑事司法实践中,事后合规激励主要体现为企业合规不起诉,即检察机关对于涉嫌犯罪的企业,责令其针对违法犯罪事实提出专项合规计划,然后作出相对不起诉决定。⑤ 事后刑事合规激励的法理基础在于有效预防犯罪,即企业通过建立有效合规体系,加强了内部合规管理,减少关联人员再犯的可能性。自最高人民检察院开展合规改革试点以来,个人信息保护领域亦积累了不少合规不起诉的成功经验。未来可以通过完善刑事合规不起诉制度,继续推动个人信息保护的刑事合规。当前个人信息保护主要依赖行政执法,因此建立事后行政合规激励制度具有迫切的实践需求。然而,在探讨其必要性和基本实现路径时,需要考虑与刑事合规不同的因素。具体而言:

1.基于合作式执法的事后行政合规

根据执法者与执法对象的不同关系,法律执行可划分为制裁式与合作式两种模式。制裁式

---

① See Neil Gunningham & Joseph Rees, Industry Self-Regulation: An Institutional Perspective, 19 Law & Policy, 392-396(1997).

② See Dennis D. Hirsch, The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?, 34 Seattle University Law Review, 457-459(2011).

③ See European Union, 2016, General Data Protection Regulation, Official Journal of the European Union, L 119(1), Arts.40, 41, 83.

④ 参见熊樟林:《企业行政合规论纲》,《法制与社会发展》2023 年第 1 期。

⑤ 参见陈瑞华:《企业合规不起诉制度研究》,《中国刑事法杂志》2021 年第 1 期。

执法主张通过提高处罚力度来增加违法成本,当违法成本高于违法收益时,理性人不会选择违法,从而形成两造对抗的执法关系。在合作式执法来看,执法对象包括道义型、理性型与非理性型 3 类,执法机构应当针对不同对象类型,从执法工具箱中选择合适的执法措施。合作式执法主张优先采取合作措施,执法机关根据执法对象的合作态度判断其类型,然后决定是否采取更严厉的执法措施。① 制裁式执法操作成本低,但违法成本与收益难以量化比较;合作式执法有助于培育合作信任关系,但实施成本高,且存在法律非平等适用的合法性质疑。在理论和实践上,关于何时采用制裁式执法、何时采用合作式执法尚未达成共识。但是,在强调原则化规制的金融、环境保护等领域,合作式执法凸显出愈来愈重要的地位,值得个人信息保护执法借鉴。

合作式执法日渐受到重视的原因是,当法律条文以原则性规定构成时,合作式执法能够培育监管与市场之间的合作信任,并促使社会各方寻求理性共识。② 原则化规制需要在规制实践中通过协商对话解决规范不确定问题。在违法行为发生后,监管部门与执法对象通过协商来确定整改措施,是实现原则性规范向具体规定转化的重要方式。原则性规范降低了行为的可预期性,在合法与违法界限模糊的合规环境中,监管部门对所有违法行为直接给予惩罚,会减损市场主体的信任。原则性规范依赖被规制主体积极预防风险,而合作式执法通过“合作—威慑”式执法方式构建适度的容错机制,有助于激发被规制主体的主观能动性。

2.个人信息保护事后行政合规的路径展开

合作式执法依赖基于动态博弈的“金字塔式”执法策略:监管部门先与执法对象协商确定守法方案,如果执法对象拒不合作,那么监管部门将逐级升级惩罚措施,威慑执法对象服从指令。③ 在个人信息保护领域,一方面,应当严惩恶性违法行为,提高个人信息保护执法威慑力;另一方面,应当开展合作式执法,通过行政和解、轻微违法不处罚等激励企业建立有效合规体系。(1)在特定案件执法中纳入行政和解。《个人信息保护法》中大量的原则性规定需要在长期产业实践中凝聚共识。然而,在共识尚未形成前,对于企业行为是否符合法律的实质要求,缺乏统一且客观的判断标准。因此,执法和解作为一种执法手段显得尤为重要,它强调执法部门与企业之间通过协商来确定个人信息保护的合规方案。如果企业未能在约定期限内完成合规计划,那么执法机关可采取更严厉的处罚措施。④ 但是,行政和解具有不确定性和契约弹性空间,存在诱发执法机关滥用裁量权的可能性。为此,有必要在适用范围与程序上进行法律控制。一方面,要妥当厘定行政和解的适用范围。在目前的证券执法中,行政和解积累了较为成熟的制度经验。根据《证券期货行政执法当事人承诺制度实施办法》第 7 条的规定,在涉嫌犯罪移送司法机关、违法行为情况严重和恶劣、证券监管机构认为不合适用执法和解的其他情形中,不得适用行政和解。这种以负面清单排除和解适用的方式,值得个人信息保护执法参考。另一方面,应通过备案审查、保障相对人程序参与权等程序机制,确保执法机构在选择执法手段时遵循比例原则、依法行政原则等

① See Ian Ayres & John Braithwaite, Responsive Regulation: Transcending the Deregulation Debate, Oxford University Press,1992,pp.35-40.

② See Julia Black, Forms and Paradoxes of Principles-Based Regulation, 3 Capital Markets Law Journal, 456 (2008).

③ 参见徐文鸣:《证券事中事后监管活动的实证分析——基于回应性执法理论的视角》,《山东大学学报》(哲学社会科学版)2022 年第 5 期。

④ 参见解志勇、石海波:《企业合规在行政执法和解中的导入研究》,《行政法学研究》2023 年第 4 期。

行政法治基本原则。(2)针对轻微违法案件适用合规减免处罚。个人信息处理活动的影响主要体现为无形价值影响,其损害形式以个体的精神恐慌为主。这种精神恐慌具有高度的主观性和相对性,使得企业在开展内部合规和权衡多元利益时面临极大的不确定性,从而有可能多次疏忽并违反法律要求。考虑到企业面临复杂的守法环境,执法体系有必要构建适度容错机制。《行政处罚法》第33条第1款规定:“违法行为轻微并及时改正,没有造成危害后果的,不予行政处罚。初次违法且危害后果轻微并及时改正的,可以不予行政处罚。”因此,在情节轻微违法行为发生后,执法机关可以通过责令改正的方式要求企业完善内部管理程序,并根据企业整改成效决定是否提升处罚强度。这种适度的容错机制有助于激发企业的主观能动性,促使其积极预防风险。当然,这涉及执法部门行政裁量权的规范行使。为规范行政处罚裁量权,并为相对人提供稳定预期,我国监管部门在食品药品安全、环境保护等领域发布了大量不予处罚、从轻处罚清单。鉴于个人信息保护领域的执法环境更为复杂,监管部门也有必要发布不予处罚与从轻处罚清单,以进一步建立健全个人信息保护事后行政合规激励机制。

Abstract: The Personal Information Protection Law of PRC requires enterprises to improve the internal management procedures, and encourages them to develop the specific management through responsibility incentives, thus forms a basic framework for corporate compliance regulation. The law has shifted from clearly defining the boundaries of behavioral obligations to guiding and motivating enterprises to improve the internal management, reflecting the abandonment of the "command-and-control" regulatory concept and the development of cooperative regulation in personal information protection. The corporate compliance regulation needs to be improved in two aspects: compliance guidance and compliance incentives. In terms of improving compliance guidance, it is necessary to establish a "risk-based regulation" compliance concept to guide enterprises to define concrete obligations in specific scenarios; at the same time, regulate the core decision-making processes of enterprises and enhance their accountability capacity. In terms of building compliance incentives, it is necessary to establish a pre-compliance incentive mechanism for personal information protection, and clarify the relationship between the compliance procedures and the harm consequences in administrative responsibility; at the same time, promote post-compliance incentives for personal information protection, and cultivate shared rationality and trust through cooperative law enforcement.

Key Words: personal information protection, corporate compliance, compliance guidance, compliance incentives

责任编辑　　谭冰霖