财经法学 No. 5，2022
pp. 81 - 94

论超大型平台独立机构的功能构造
——以《个人信息保护法》第58条为中心

韩　阳*

内容提要：《个人信息保护法》第58条第1项规定超大型平台企业应成立主要由外部成员组成的独立机构对个人信息保护情况进行监督，目前存在三种制度设计方案。第三方独立机构方案比较优势不明显，不符合风险预防理念，难以承载监督功能期待，因此应当被舍弃。管理监督型独立机构方案属于日常性合规管理模式，是董事会对经理层的管理监督，独立机构在董事会领导下开展活动，无法解决合规动力问题，难以厘清董事会与执法机构之间的紧张关系。决策监督型独立机构方案属于危机性合规整改模式，是执法机构对董事会的整改督导，组建董事会专门委员会，依托独立董事进行内部控制，但独立董事法律责任模糊，容易造成董事会负担过重。两种方案各有优劣侧重，应当区分问题场景分别应用，实现对公民个人信息的系统性和持续性保护。

关键词：超大型平台　独立机构　管理监督　决策监督

一、问题的提出

为加强超大型平台监管，我国《个人信息保护法》新增了独立机构这一制度要求。《个人信息保护法》第58条第1项规定，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，应当按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督。问题随之而来：独立机构的功能定位、人员构成、权利义务和法律责任应如何设计？怎样保持该机构的独立性？如何实现有效监督？本文尝试对此进行探索。

为什么要求超大型平台成立独立的监督机构？与个人信息保护负责人是什么关系？缘何独立

* 韩阳，北京大学法学院博士研究生。

机构主要由外部成员组成呢？对于这些问题，立法资料显示“有的部门、专家建议，强化超大型互联网平台的个人信息保护义务，并加强监督”，全国人大宪法和法律委员会经研究建议增加这一款。〔1〕2021 年 8 月 20 日，经过三次审议，十三届全国人大常委会第三十次会议表决通过了《个人信息保护法》，全国人大常委会法工委经济法室副主任杨合庆对《个人信息保护法》进行了解读。他表示：“为了提高大型互联网平台经营业务的透明度，完善平台治理，强化外部监督，形成全社会共同参与的个人信息保护机制……个人信息保护法对这些大型互联网平台设定了特别的个人信息保护义务。”〔2〕由此可见，我国立法机关将独立机构的功能定位为外部监督，通过多元主体参与构建平台治理的开放式关系结构。

从法律条文看，独立和监督是该机构的两个显著特征，外部是对组成人员的要求。监督是该机构的功能定性，是设计这一机构的出发点和落脚点。独立性包含组织独立、职权独立和人员独立三个方面。只有在监督者和监督对象都明确的前提下，是否独立才能够最终研判。如何实现独立监督呢？学界和实践中存在三种方案，分别是第三方独立机构方案、管理监督型独立机构方案和决策监督型独立机构方案，以下分别进行讨论。部分方案内容较少，本文尝试进行拓展并做利弊分析。

二、第三方独立机构方案

在《个人信息保护法》生效前，部分超大型平台企业已经进行了初步尝试。腾讯在 2021 年 10 月 15 日公开招募外部成员，组建个人信息保护外部监督委员会，文字表述为“第三方独立监督机构”，职责包括独立评议腾讯公司及各产品隐私保护相关工作、提出指导和修改建议等。“委员会首批成员为 15 个人左右，计划包括法学专家、技术专家与行业协会等个人信息保护领域的专业人士，也将涵盖律师、媒体等其他公众。首批成员将通过公开招募和定向邀请等方式产生。”〔3〕携程在 2021 年 10 月 25 日发布公告，决定近期成立“个人信息保护外部监督专家团”，同样表述为“第三方独立机构”。〔4〕在外部监督的功能定位下，超大型平台希望通过第三方独立机构的形式实现外部监督效果，将独立性理解为“外部独立”，监督机构独立于本平台企业。但这种做法比较优势并不明显，不符合风险预防的治理理念。

第一，《个人信息保护法》第六章专门规定了履行个人信息保护职责的部门，这些职能部门完全独立于企业，属于纯粹外部监督的国家机构。无论立法目的追求的是“独立性”或是“监督性”，负有监管职责的国家机关都是最佳主体，而不是所谓的第三方独立机构。近年来行政执法强调柔性执法和治理导向，存在许多企业发声和公众参与的合法渠道。反观这些所谓的独立机

〔1〕 参见《全国人民代表大会宪法和法律委员会关于〈中华人民共和国个人信息保护法（草案）〉修改情况的汇报》。

〔2〕 朱宁宁：《8 章 74 条，个人信息保护法来了！权威解读十大亮点》，载 https://mp.weixin.qq.com/s/Y-031EBzOsbbN2JAEcOGBQ，最后访问时间：2022 年 7 月 23 日。

〔3〕《这是一封来自鹅厂隐私官的邀请函，请查收！》，载 https://mp.weixin.qq.com/s/2ZvcExeY_l-J3dfw02zTFg，最后访问时间：2022 年 7 月 23 日。

〔4〕 参见《携程“个人信息保护外部监督专家团”招募公告》，载 https://view.inews.qq.com/a/20211025A093AW00，最后访问时间：2022 年 7 月 23 日。

构，实际上难以摆脱超大型平台的干扰，平台企业主导之下的民主参与和监督强度都存在问题。用户代表或公众代表的产生，专家学者的挑选，都有可能被超大型平台把持，使所谓的独立监督机构沦为平台权力的装饰。

第二，即便追求平台治理的多元参与，实际上也并无必要。现实中已经广泛存在着第三方独立机构，各类行业协会、学会智库和科研高校等等，如在 APP 专项整治活动中发挥作用的中国网络空间安全协会，每年发布个人信息保护测评报告的北京大学互联网法律中心。这些机构或独立存在，或由政产学研媒一同发起成立，各大头部平台企业也参与其中。它们定期发布研究报告，组织企业调研、立法研讨和独立监督，实际上已经发挥了社会监督的客观作用。这些社会组织通过内部章程对成员形成约束力，通过法律程序获得登记备案，不需要专门立法予以合法性确认。这些社会组织的经费人员更具有独立性，它们通过声誉机制和竞争机制进行自我监督，相较企业自设机构具有一定的制度优势。

第三，外部监督无法实现事前事中监管，难以有效影响超大型平台企业决策。如果按照两家企业的制度设想展开，独立机构对超大型平台进行形式监督，仅仅作出指导、提出建议和咨询培训，那么独立机构极容易沦为装饰企业形象的花瓶，监督功能将被完全掏空。独立机构无法深入平台企业内部决策，否则就将与外部监督的职能定位相冲突。超大型平台企业的各种业务和不同流程都与个人信息有关，个人信息被滥用有时候只是一个最终结果，更多问题可能出在事前决策和事中执行。尤其是很多敏感个人信息，如生物识别信息，一旦被泄露滥用将会给自然人带来不确定风险。有学者提出：“区别于传统的‘危险’，个人生物识别信息应用风险具有不确定性与复杂性，因果关系具有模糊性与非线性，损害具有严重性与不可逆性，因此政府监管理念应当从消极的‘危险消除’向积极的‘风险预防’转变。”〔5〕

三、管理监督型独立机构方案

该方案由张新宝教授提出，主张“作为企业内部的‘独立监督机构’，主要是指独立于企业的日常经营管理机构（如总经理）、产品或者服务研发推广机构等业务部门，因为这些机构和部门往往会以利润导向进行管理和经营而忽视个人信息保护”〔6〕。该方案下独立机构包含两项具体职责：其一，监督大型互联网平台企业自身的个人信息保护合规情况；其二，监督大型互联网企业对商业用户的个人信息处理活动予以规范的合规情况。〔7〕除此之外，独立机构在董事会的领导下，还有提出建议和合规指导的功能。超大型平台的业务部门是该方案的预设监督对象，本质是董事会对经理层的管理监督。数据合规在我国仍处于发展初期，该方案有助于专家参与企业合规制度建立，同时制度上防范经理层和业务部门的数据滥用行为，方案内容丰富具有很强的操作性和执行性。在讨论独立机构与国家个人信息保护部门的关系时，张新宝教授主张：“独立监督机构对企业个人信息保护事项作出的决定或者提出的鉴定意见，原则上将得到国家个人信息保护

〔5〕 于洋：《论个人生物识别信息应用风险的监管构造》，载《行政法学研究》2021 年第 6 期，第 111 页。
〔6〕 张新宝：《大型互联网平台企业个人信息保护独立监督机构研究》，载《东方法学》2022 年第 4 期，第 44 页。
〔7〕 参见前引〔6〕，张新宝文。

部门的认可。在发现企业在个人信息保护方面存在重大隐患或者严重违法情形时，独立监督机构应当及时向企业的权力机构提出意见和建议。企业权力机构拒绝接受的，经独立监督机构多数成员表决同意，应将相关情况报告国家个人信息保护部门。”〔8〕这一制度设计极大增强了独立机构的实际权力，仿佛达摩克利斯之剑一样悬在超大型平台企业头顶。但是产生两个问题需要解释：第一，如果独立机构受董事会领导，为什么决定和鉴定意见要征得监管部门认可，为什么可以越过董事会，直接向监管部门报告；第二，如果独立机构照此运行，会不会干扰企业的自主经营活动。

在规制理论中，该方案属于内部管理型规制理论（management-based regulation）〔9〕的实际运用，“实际上是行政权对企业内部治理的介入，在实质上构成对企业经营自主权的限制”〔10〕。对于内部管理型规制，国外学者将生产流程划分为规划、执行和产出三个部分，在不同阶段采取的规制策略，被称作内部管理型规制、技术标准规制（technology-based regulation）和绩效标准规制（outcome-based regulation）。根据内部管理型规制，公司应制定符合一般标准的计划，以促进有针对性的社会目标。监管标准规定了每个计划应该具备的要素，如危险识别、风险防范措施、监测纠正程序、员工培训政策，以及其他社会目标评估和完善公司管理的具体措施。〔11〕“内部管理型规制不规定特定的技术要求或绩效结果，而是要求企业针对行政目标，制定适合自身的内部经营计划、管理流程及决策规则，从而将社会价值内部化。”〔12〕这一规制类型属于元规制（meta regulation）的典型类型，与自我规制具有高度关联性。“元规制是指外部规制者有意促使规制对象本身针对公共问题，作出内部式的、自我规制性质的回应，来要求或塑造规制对象的自我规制。”〔13〕

结合内部规制理论，该方案具有三点积极意义：第一，针对个人信息风险，应该采用风险预防的规制策略。“互联网的复杂结构以及大数据处理过程随机性、相对性和模糊性特征，表明数据主体基于个人信息与数据控制者建立的信息关系影响因素存在高度的不确定性。传统规制模式以规则为规制工具，通过行为和结果的确定性联系进行危险排除，并不符合数字时代信息分享的风险特征。”〔14〕第二，当风险不明、标准不清时，实际上难以判断个人信息是否被滥用泄露，事后监督难以挽回实际损失。需要深入平台企业内部，对个人信息管理体系进行优化改造，政府规制视角应该由外入内。第三，个人信息保护问题异质性强，平台、部门和流程之间都不一样，需要编制细密的行动规范。但是，个人信息保护法律制度建立初期，诸多制度细节、技术标准和行

〔8〕 前引〔6〕，张新宝文，第 48 页。

〔9〕 也有学者将其翻译为“以管理为基础的规制”或“基于管理的规制”。参见洪延青：《“以管理为基础的规制”——对网络运营者安全保护义务的重构》，载《环球法律评论》2016 年第 4 期；高秦伟：《社会自我规制与行政法的任务》，载《中国法学》2015 年第 5 期。

〔10〕 孔祥稳：《论个人信息保护的行政规制路径》，载《行政法学研究》2022 年第 1 期，第 144 页。

〔11〕 See Cary Coglianese & David Lazer, Management-Based Regulation: Prescribing Private Management to Achieve Public Goals, 37 *Law & Society Review* 694 (2003).

〔12〕 谭冰霖：《论政府对企业的内部管理型规制》，载《法学家》2019 年第 6 期，第 75 页。

〔13〕〔英〕罗伯特·鲍德温、马丁·凯夫、马丁·洛奇：《牛津规制手册》，宋华琳等译，上海三联书店 2017 年版，第 167 页。

〔14〕 谢尧雯：《基于数字信任维系的个人信息保护路径》，载《浙江学刊》2021 年第 4 期，第 82 页。

业要求都需要进一步明确。因此，应将规则自由裁量权下放给企业，监管机构不宜采取硬标准强要求。

但是，运用内部规制理论分析建构超大型平台独立机构，存在固有缺陷难以克服。内部管理型规制本质上仍是一种外部监督，无法解决合规动机问题。经过与监管机构的沟通确认，企业制定实施了各类内部管理制度，既有可能出于提升公司绩效考虑，也可能是为了应付检查粉饰门面。企业并非自发遵守合规计划，而是考虑制度成本、外界压力和管理层意见。制度运行成本较低，契合企业盈利模式，得到管理层的支持，内部管理制度可以有效运行；但如果遇到任何一个障碍，内部管理制度运行就可能是“部分的、象征性和半心半意（half-heated）”。〔15〕监管者真正应该关心的是企业管理的实际行动，而不是浮于表面的规章制度，“管理远比管理体系重要”〔16〕。对企业行为的规制，仅仅停留在管理制度上是不够的，需要干预企业管理层或控股股东的合规动机。在这个层面上独立机构的监督职能或许更有意义。

2019年7月美国联邦贸易委员会（FTC）对脸书（Facebook）达成新的和解令，以惩罚脸书违反2012年和解令中“禁止虚假陈述”的要求。除了开具50亿美元的天价罚单，2019年和解令还要求脸书改变其董事会构成，设立专门独立隐私委员会。它的所有成员都必须是独立董事，由独立提名委员会产生，每年至少召开4次会议。有权任命或免职隐私合规官，每12个月审核隐私合规官提交的隐私计划执行情况书面说明。有权任命或免职第三方隐私评估机构，每季度应在没有管理层出席的情况下与其举行会议。每季度审核管理层提交的简报，内容涵盖隐私计划状态、和解令执行情况和存在重大风险情况等等。〔17〕美国联邦贸易委员会的执法意图十分明确，约束限制管理层尤其是控股股东扎克伯格在隐私方面的权力。委员会委员罗希特·乔普拉（Rohit Chopra）发表声明称，脸书通过对外销售用户的行为数据换取广告收入，有强烈的动机获取越来越多的用户数据。只要广告商愿意为用户消费特定内容付费，像脸书这样的公司就有动机以影响用户的心理状态和实时偏好的方式来管理内容。作为一家上市公司，脸书需要与利润丰厚的第三方开发者保持合作，实现公司利益的最大化。〔18〕委员会主席乔·西蒙斯（Joe Simons）和委员诺亚·约书亚·菲利普斯（Noah Joshua Phillips）、克里斯汀·S·威尔逊（Christine S. Wilson）发布声明称，该命令消除了扎克伯格单方面做出隐私决策的能力，赋予业务部门、首席隐私官和隐私委员会相关责任。尽管没有移除扎克伯格对董事会的全部控制权力，但明显地削弱了他的权力，这是迄今为止世界上没有哪个监管机构能做到的。〔19〕

---

〔15〕 See Christine Parker & Vibeke Lehmann Neelsen, Do Businesses Take Compliance Systems Seriously? An Empirical Study of Implementation of Trade Practices Compliance Systems in Australia, 30 *Melbourne University Law Review* 441 (2006).

〔16〕 前引〔13〕，罗伯特·鲍德温、马丁·凯夫、马丁·洛奇书，第154页。

〔17〕 See United States of America v. Facebook Inc, Case No. 19-cv-2184 (United States District Court for the District of Columbia. 2019).

〔18〕 See Rohit Chopra, Dissenting Statement of Commissioner Rohit Chopra, In re Facebook, Inc. Commission File No. 1823109 (July 24, 2019), available at https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf, last visited on Mar. 3, 2022.

〔19〕 See Joe Simons, Noah Joshua Phillips & Christine S. Wilson, Statement of Chairman Joe Simons and Com-missioners Noah Joshua Phillips and Christine S. Wilson In re Facebook, Inc. (July 24, 2019), available at https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf, last visited on Mar. 3, 2022.

通过分析脸书 2012 年和 2019 年两宗案件可知，如果没有触及超大型平台的盈利模式，以及管理层或控股股东对个人信息利用的绝对控制，单纯对超大型平台进行事后监管和流程改造，无法对平台企业的合规动机进行根本影响。因此，需要监督的对象实际是超大型平台的管理层或控股股东。事实上，2012 年和解令最终确定的 4 个月后，脸书就允许第三方开发人员违规使用用户个人信息。〔20〕

由此可见，超大型平台独立机构的制度建构，不仅需要引入政府规制理论，而且应该引入公司治理视角。超大型平台企业的迅速崛起只是近二十年的事情，不少创始人仍然牢牢掌控已经上市的平台企业，并未实现所有权与经营权的分离。脸书的公司结构为 B 级股股东提供了“超级投票权”，扎克伯格的投票决定了董事选举和其他需要股东投票的事项。〔21〕“脸书股东厌倦了扎克伯格，但对他们无能为力。”〔22〕我国存在类似的情况，“作为企业家的发起人或创始股东珍视控制权以实现自己的愿景和抱负，这种对控制权的珍视体现为对发起人或创始股东权利的特殊安排”，如 B 站的双层股权结构、京东的投票委托权和阿里巴巴的合伙人制度等等。〔23〕相较于美国，中国互联网企业模式创新有余而技术创新不足，更加依赖个人信息和人力资源投入。具有类似的公司结构，承担着巨大的利润压力，依靠大量采集个人信息以维持商业运转，我国超级平台管理层或控股股东的合规动力更加匮乏。

四、决策监督型独立机构方案

为加强对管理层或控股股东的控制，不少国家规定董事会负责内控机制建设，赋予董事一定的法律义务。如日本《公司法》规定了董事构建内控机制的任务，《公司法实施规则》规定了构建内控机制的具体内容。〔24〕我国也有学者建议：“想让外部的监督发挥实效，就必须通过内部的决策机构。而内部决策机构最好的做法就是仿效独立董事的相关制度——在董事会下面设立一个主要由独立董事承担监督作用的个人信息保护专门委员会。”〔25〕如果公司董事会全部由管理层组成，那么董事会的存在就没有实际意义，董事会就变成了一个拥有高级头衔的管理委员会了。决策监督型独立机构方案下，我国不少学者建议将外部监督成员理解为公司的独立董事，独立董事组成独立机构负责对企业的个人信息保护作出判断和监督。〔26〕该方案如何展开，具有哪些优势

---

〔20〕 See FTC Imposes $ 5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, Federal Trade Commission (July. 24, 2019), available at https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions, last visited on Mar. 3, 2022.

〔21〕 参见前引〔18〕，Rohit Chopra 文。

〔22〕 Michael Hiltzik, Facebook Shareholders are Getting Fed Up with Zuckerberg but Can't Do Anything about Him, Los Angeles Times: Business (Apr. 16, 2019), available at https://www.latimes.com/business/hiltzik/la-fi-hiltzik-mark-zuckerberg-facebook-20190416-story.html, last visited on Mar. 13, 2022.

〔23〕 参见汪青松、宋朗：《合规义务进入董事义务体系的公司法路径》，载《北方法学》2021 年第 4 期。

〔24〕 参见梁爽：《内部控制机制的法律化路径——以日本法上董事内部控制义务为视角》，载《金融法苑》2015 年第1 期。

〔25〕 隐私护卫队：《外部机构如何监督企业个人信息保护？许可：不能存在经济依附》，载 https://www.sohu.com/a/509672335_121258695，最后访问时间：2022 年 7 月 23 日。

〔26〕 参见张平主编：《中华人民共和国个人信息保护法理解适用与案例解读》，中国法制出版社 2021 年版，第 225 页；龙卫球主编：《中华人民共和国个人信息保护法释义》，中国法制出版社 2021 年版，第 260 页。

与弊端？现有文献没有对此进行讨论，本文尝试进行探索展开。

（一）方案的理论渊源

该方案与公司治理中的内部控制理论有关。内部控制在会计学和审计学中较为常见，近年来随着法学界对企业合规的关注，逐渐进入法学视野。“内部控制起源于企业财务舞弊、财务失败事件的不断发生，内部控制的发展与美国公司会计造假、破产倒闭事件周期性的发生有着密不可分的关系，每一轮的公司财务舞弊、破产倒闭事件都促进了内部控制理论的发展。”〔27〕例如美国《反海外贿赂法》（FCPA）要求证券发行者必须设计和维持有效的内部会计控制系统。〔28〕我国法律对内部控制理论也有类似应用，例如2021年6月中国人民银行发布的《中华人民共和国反洗钱法（修订草案公开征求意见稿）》第3章“反洗钱义务”第27条第3款规定：“金融机构应当通过内部审计或者独立审计等方式，监督检查反洗钱内部控制制度的有效实施，金融机构的负责人对反洗钱内部控制制度的有效实施负责。”

个人信息保护与企业财务管理存在较大相似性，都涉及企业的不同环节和各个流程，与企业经营模式和利润收支息息相关，关乎企业的生死存亡。尤其在消费者信息隐私意识觉醒的今天，对于超大型平台企业而言，个人信息保护不仅应是其努力控制的成本线，而且应该是严格遵守的生命线。因此，类比财务风险管理，个人信息风险控制完全可以应用内部控制理论。正如学者所说：“内部控制发展到今天，已经演变成一种过程，内化于企业的各个流程、各个环节，和企业的各类人员相联系，但从内部控制的对象和目标来看，其本质并没有发生变化，依然是一种风险控制活动。”〔29〕内部控制与风险管理属于一体两面，本质上都是对风险的有意控制。“内部控制就是控制风险，控制风险就是风险管理。”“内部控制主要是从风险控制的方式和手段说明风险控制的，风险管理就是从风险控制的目的来说明风险控制的。”〔30〕为强调对管理层和控股股东的力量制衡，避免风险管理和企业管理概念混淆，本文采用内部控制的概念。

对于内部控制的定义，美国国家金融欺诈信息委员会（Treadway委员会）下属的“发起组织委员会”（COSO）〔31〕发布的《COSO内部控制—综合框架（2013）》指出，内部控制是一个由实体董事会、管理层和其他人员实施的过程，旨在为实现运营、报告和合规相关目标提供合理保证。合规目标与遵守实体法律法规有关。这一框架包含控制环境、风险评估、控制活动、信息交流和监控活动五个组成部分。〔32〕我国财政部、证监会、银监会等五部委于2008年5月发布的《企业内部控制基本规范》第3条规定：“本规范所称内部控制，是由企业董事会、监事会、经理

〔27〕 李维安、戴文涛：《公司治理、内部控制、风险管理的关系框架——基于战略管理视角》，载《审计与经济研究》2013年第4期，第5页。

〔28〕 See The Foreign Corrupt Practices Act of 1977 § 15 U. S. C. § 78dd-1, et seq.

〔29〕 前引〔27〕，李维安、戴文涛文，第6页。

〔30〕 谢志华：《内部控制、公司治理、风险管理：关系与整合》，载《会计研究》2007年第10期，第41页。

〔31〕 COSO英文全称为Committee of Sponsoring Organizations of the Treadway Commission。COSO在美国成立于1985年，旨在赞助国家金融欺诈信息委员会（Treadway委员会）。Treadway委员会最初由位于美国的以下五家主要专业会计协会和机构发起和共同资助：美国注册会计师协会（AICPA）、美国会计协会（AAA）、国际财务执行官（FEI）、内部协会审计师（IIA）和管理会计师协会（IMA）。

〔32〕 See The Committee of Sponsoring Organizations of the Treadway Commission (COSO), COSO Internal Control-Integrated Framework (2013) (May 14, 2013), available at https://assets.kpmg/content/dam/kpmg/pdf/2016/05/2750-New-COSO-2013-Framework-WHITEPAPER-V4.pdf, last visited on Feb. 13, 2022.

层和全体员工实施的、旨在实现控制目标的过程。内部控制的目标是合理保证企业经营管理合法合规、资产安全、财务报告及相关信息真实完整，提高经营效率和效果，促进企业实现发展战略。”企业控制目标的实现需要由股东会、董事会、监事会和管理层等各个组织机构共同完成。构建合规制度体系是内部控制目标，无论由董事会或监事会设置独立机构，它们开展的内部监督活动都属于风险控制的内部过程。

该理论强调应发挥董事会内部控制的主导作用，例如《上海证券交易所上市公司内部控制指引》第 4 条规定：“公司董事会对公司内控制度的建立健全、有效实施及其检查监督负责，董事会及其全体成员应保证内部控制相关信息披露内容的真实、准确、完整。”比较法上，韩国存在类似的“合规监查人”制度。“合规监查人通常从公司内部的董事或业务执行负责人中选任，其虽由董事会任命，但却独立履行职务，其业务活动不受董事会或代表董事的干预。为了保障其独立性地位，韩国《金融公司治理结构法》第 30 条要求金融公司应当通过章程保障合规监查人独立履行职务，并为其履行职务提供必要的资料和信息；对合规监视人的任免虽由公司自主决定，但须在作出决定之日起 7 天内向金融委员会报告。公司未按规定设置合规监视人或未按照合规要求进行报批和运营的，根据该法第 43 条第 16—22 款的规定，可对其处以罚款。”〔33〕

美国学者提出了应由董事会承担内部控制最终责任的两点理由：第一，企业高管有可能扭曲信息流动。解决信息不对称问题，创造竞争性的信息来源。第二，存在管理机会主义问题。管理层面临业绩压力，任期薪酬与企业盈利高度相关。在一笔违反公司政策或法律规则的交易中，预期的利润通常是巨大、现实和生动的。相比之下，从经理的角度来看，违反公司政策或法律规则可能造成的损失往往微不足道、苍白、非常遥远，尤其是考虑到发现的可能性极低时，情况更是如此。董事们不寻求晋升，通常不负责短期利润决策判断，因而对于公司整体和长远利益更加看重。〔34〕脸书案件体现了该学者的公司治理思路，2019 年和解令创造了加强脸书隐私监管的四个信息流，建构了一种重叠的合规监督渠道（overlapping channels of compliance），以提高风险防控效率。〔35〕为加强对某一重要事项的整体管理，董事会设置专门委员会的做法在实践中已经很常见。如很多上市公司在董事会设立社会责任专门委员会和环境保护专门委员会。〔36〕

（二）设在董事会下而不是监事会下

内部控制职责的权能配置，实际上与不同国家公司法规定的组织结构有关。“英美法国家实行的主要是以外部董事为核心的监督制度，它与我国的独立董事制度相似。在以德国为代表的大陆法国家，实行的主要是以监事会为核心的监督制度。”〔37〕我国《公司法》规定董事会和监事会两个组织机构负责内部监督职能。有的学者认为转换到中国背景下监事同样负有内部控制义务。〔38〕我国《公司法》虽然没有明确规定外部监事制度，但是部分企业早已开始探索实施，如

〔33〕 赵万一：《合规制度的公司法设计及其实现路径》，载《中国法学》2020 年第 2 期，第 76 页。

〔34〕 See Melvin A. Eisenberg, The Board of Directors and Internal Control, 19 *Cardozo Law Review* 237, 250 (1997).

〔35〕 参见前引〔19〕，Joe Simons、Noah Joshua Phillips、Christine S. Wilson 文。

〔36〕 参见蒋大兴：《公司社会责任如何成为“有牙的老虎”——董事会社会责任委员会之设计》，载《清华法学》2009 年第 4 期。

〔37〕 高旭军：《对我国上市公司“双核心监督机制”的反思》，载《东方法学》2016 年第 2 期，第 58 页。

〔38〕 参见邢会强：《上市公司虚假陈述行政处罚内部责任人认定逻辑之改进》，载《中国法学》2022 年第 1 期。

中国人民银行2002年就曾发布《股份制商业银行独立董事和外部监事制度指引》。有学者提出独立董事的监督是决策中的监督，监事会的监督体现为事后监督。〔39〕以上观点和实践都具有借鉴意义，存在两个内部监督机关的情况下，董事会和监事会都可以承担个人信息保护的内部控制职责。需要进一步思考的是，为落地实施《个人信息保护法》，是否需要《公司法》相应修改，董事会和监事会哪一个组织更具有设置独立机构的制度潜力。

本文认为在坚持现有公司法框架下，独立机构更适合设置在董事会中，主要成员由独立董事担任。为了解决监事会存在的问题，我国引入了独立董事制度。公司监事会作为专门监督机构，普遍存在“监事会地位低下、资源匮乏，职工监事制度徒具其形，监事缺乏适当的考核和激励机制，与独立董事关系不清、叠床架屋，受制于高管控股股东”等问题。〔40〕不同学者总结的原因或有出入，但是监事会孱弱无力确是现实，无力对抗控股股东实施有效监督。我国《公司法》规定监事会由股东代表和职工代表组成，职工代表的比例不得低于三分之一，意图加强股东和雇员对公司的自我监督。但股东代表产生受制于控股股东，职工代表履职遭雇佣关系掣肘。即便允许外部监事加入，也难以改变监事会的固有缺陷。独立机构要求主要由外部成员组成，这与监事会的人员比例要求也存在出入。董事会拥有解聘或聘任管理层和制定规章制度等事项的决定权，可以有效建构个人信息保护内控合规体系。但是监事会仅具有建议、质询和调查等权利，只能列席董事会会议，没有投票表决权和否决权。我国超大型平台企业多赴美股和港股上市，就个人信息保护问题对董事会进行改造，与英美公司法传统不存在较大差异，更有利于企业降低合规成本。

（三）独立董事需要平衡股东利益与公共利益

独立机构由独立董事构成，独立董事实际开展监督活动，但是独立董事应该对谁负责，却鲜有学者深入研究。有专家观察到存在利益冲突的可能，有针对性地提出“如果认为独立监督机构对社会公众负责，公司的发展利益或将不作为独立监督机构考虑的范畴，有可能导致公司发展利益受损”〔41〕。这些观察实际上点出了问题的实质，独立董事应该对公共利益负责，还是对企业利益和股东利益负责？《上市公司独立董事规则》第5条规定独立董事应该维护公司整体利益，尤其要关注中小股东的合法权益不受损害。但是超大型平台收集了大量的公民个人信息，即便个人信息处理者投入了汗水劳动，个人信息蕴含的人格利益仍然属于公民或用户个人。空泛地说，公司利益、股东利益与社会公共利益当然是一致的，企业违反法律规定侵犯公共利益受到法律制裁，也会损害企业利益和股东利益。“但这个观点其实只是体现了一种‘大家好才是真的好’的良善价值导向，在逻辑上就如同个体利益和群体利益可以两全的论断一样脆弱，如果真的可以两全就不会有损公肥私和牺牲小我完成大我的问题。”〔42〕事实上滥用公民个人信息的现象已经如此普遍，大量的违法行为并没有被发现惩处，有些人甚至怀疑是否还有继续保护的必要。因此，实践中公司利益、股东利益与公共利益广泛存在着利益冲突。努力追求私人利益，既有可能成为创

〔39〕 参见施天涛：《让监事会的腰杆硬起来——关于强化我国监事会制度功能的随想》，载《中国法律评论》2020年第3期。

〔40〕 参见郭雳：《中国式监事会：安于何处，去向何方？》，载《比较法研究》2016年第2期。

〔41〕 虞伟：《个保法要求建外部独立监督机构，互联网平台为何按兵不动》，载https://xw.qq.com/cmsid/20211111A009I900，最后访问时间：2022年7月23日。

〔42〕 前引〔23〕，汪青松、宋朗文，第81页。

新创业的动力源泉，也有可能是公地悲剧的罪魁祸首。盲目乐观与有意回避都不可取，在流通利用中个人信息才能发挥实际价值。真正值得思考的是，如何通过法律规则调整实现不同利益平衡。

传统公司法理论认为董事仅对股东利益负责，追求股东利益最大化。基于公司所有权与经营权分离的现实情况，股东选举产生董事负责实际经营，股东与董事之间属于委托代理关系，董事对股东负有信义义务，通说认为至少包含忠实义务和勤勉义务。尽管从 19 世纪 30 年代开始，美国学界开启的企业社会责任讨论一直延续至今，但是这一框架仍是公司法的基本理论模型。正如前美国特拉华州最高法院首席大法官小利奥·E·斯特林（Leo E. Strine，Jr.）所说，“这些公司的董事会认为，他们所管理的共和国应该对唯一公民忠诚，而这些公民被称为股东。这些公司的董事会并不认为自己对其他选区有任何国家的忠诚度，他们认为自己是股权资本共和国的民选官员。”〔43〕但是董事追求股东利益并非没有限度，必须遵守法律的各项要求，意味着对于法律强制性规定事项，董事不能进行成本收益比较，这实际上在法律框架内限制了股东利益。伴随着美国公司所有权与经营权的分离，众多学者提出应该考虑企业的社会责任，公司董事会不仅要对股东利益负责，而且要考虑消费者、社区、雇员、客户和环境保护等非股东利益，由此产生了诸如利益相关者理论、公司公民理论、公司善治运动等理论思潮。〔44〕公司生产经营会产生各种社会成本，污染环境、劳工、金融风险等问题都需要公司经营者认真考虑。立法者希望通过成文立法解决这些问题，规定企业相应的法律义务，我国《个人信息保护法》也是如此。企业毕竟不是政府，企业存在的根本目的仍是追逐利润。曾经有人建议在公司董事会设立代表不同群体利益的公益董事，有学者评论说，即便全部董事追求公司利益最大化，都不一定可以实现意见统一。如果董事会充斥着目标不同相互竞争的支持者，那将是大多数管理者的噩梦。〔45〕如果赋予企业过多的公共责任，可能会将企业经营变成政治活动，董事之间的实质性利益冲突会导致公司无法经营。由此可知，如同公司一样，董事会既不可能彻底坚持“股东至上”，也无法完全替代政府追求公共利益，坚持维护股东利益兼带平衡公共利益才是现实选择。在个人信息保护问题上同样如此，个人信息只有在聚合、加工和利用之后才能发挥最大价值，平台企业的产品创新和商业开发在其中发挥了不可替代的作用，规范利用是最终目的，违规惩戒只是手段。因此，独立机构作为董事会的下设机构，需要平衡股东利益和公共利益。部分学者认为它不对个人信息处理者负责、单纯维护公共利益、应该保持中立性的观点是错误的。

独立董事作为独立机构的成员，应追求实现企业利益，我国《公司法》第 147 条和《上市公司独立董事规则》第 5 条均有直接规定。与《公司法》立法目的不同，《个人信息保护法》不要求独立董事关注中小股东的合法权益，而是强调他们对个人信息保护情况进行有效监督，主要关注广大力量分散的公民个人信息权益，本质上属于一种利益相关者权益。这部分利益与中小股东利益风险偏好存在明显不同，但是它们都依附在公司整体利益之上。无论是维护中小股东利益，

〔43〕 Leo E. Strine Jr.，Corporate Power is Corporate Purpose II：An Encouragement for Future Consideration from Professors Johnson and Millon，74 *Washington and Lee Law Review* 1，13（2017）.

〔44〕 参见施天涛：《〈公司法〉第 5 条的理想与现实：公司社会责任何以实施?》，载《清华法学》2019 年第 5 期。

〔45〕 See Alfred F. Conard，Reflections on Public Interest Directors，75 *Michigan Law Review* 941，950（1977）.

还是为了公民个人信息权益，法律为分散的利益群体选派代表，都试图打破控股股东的非对称权利结构，努力干预影响公司决策。二者在规制思路上是相似的，这是嫁接独立机构职能与独立董事职责的基础。股东利益、公司利益和公共利益，三者在合规层面是一致的。法律底线不容利益权衡，遵纪守法保障企业长远。这解释了为什么设置独立机构是构建合规体系的一部分，为什么独立机构与合规体系共同组成《个人信息保护法》第58条第1项。

（四）独立董事承担的法律义务之性质

结合我国《公司法》，独立董事的这种内部控制行为属于什么法律义务？我国《公司法》第147条规定董事对公司负有忠实和勤勉义务，《上市公司独立董事规则》第5条规定独立董事对上市公司及全体股东负有诚信与勤勉义务。这里出现了三种义务类型：忠实义务、诚信义务和勤勉义务，内部控制与三者是什么关系？法律义务这一概念本质要求主体行为符合法律规定，文字意义上所有部门法规定的各项法律义务都属于“合规义务”，但是某一种“合规行为”能否成为独立具体的法律义务就值得讨论了。这些新增的合规义务是否属于信义义务？或者它们可以成为一种新的“合规义务”？存在独立的内部控制义务吗？目前主要存在三种观点：第一，内部控制行为属于忠实义务或诚信义务的一种。诚信义务是否属于一种单独的信义义务类型，在美国公司法上存在着“三分法”和“二分法”的争议。本文无意对此进行明确区分，故将忠实义务与诚信义务进行并列。有学者提出，美国法上在董事违反内部控制机制建构义务的案例中，如Caremark案以及Stone案，法院一般认为董事故意忽视自身职责，往往会判定董事违反忠实义务。〔46〕第二，内部控制行为属于勤勉义务或注意义务的一种。有学者提出：“就履行个人信息保护法定义务而言，在学理上属于公司董事、高管应当履行的勤勉义务，即公司管理者应当保障公司能够切实履行法律规定的保护个人信息的义务，从而维护公司的利益，避免公司因义务不履行而遭受不利的法律后果，诸如，损害赔偿、行政处罚，甚至刑事处罚。”〔47〕有学者认为内部控制义务是董事勤勉义务的具体化和内在化，认为“对企业发生的重大事件或事故，即使是无需董事亲自决策和具体实施的小事直接引起的，如果该重大事件或事故与内部控制的不健全有关联，是和未能建立健全能尽早发现纠正违法违规事件的源头原因，防止事件发生的公司内部控制有关联，在一定条件下，也应认定董事违反了内部控制义务，董事应对公司承担相应的损害赔偿责任”〔48〕。还有学者分析德国公司法，论证从业务执行机构的谨慎义务中引申出来的合法性管控义务可以成为合规组织义务的法律基础。〔49〕第三，内部控制属于一种特殊的合规义务，与董事信义义务并列。有学者认为“董事信义义务的产生原因系董事与公司及股东间的委托代理关系和利益冲突，旨在减少公司治理中的代理成本。而董事的合规义务源于公司行为的合法性要求从组织层面向个体层面的下沉，旨在减少公司经营中的社会成本”，两种法律义务的产生原因存在根本不同，因此势

〔46〕 参见梁爽：《董事信义义务结构重组及对中国模式的反思——以美、日商业判断规则的运用为借鉴》，载《中外法学》2016年第1期。

〔47〕 张怀岭：《公司治理视域下个人信息保护的实现路径——以〈公司法〉第147条的具体化为中心》，载《财经法学》2018年第5期，第28页。

〔48〕 刘惠明、祁靖：《内部控制义务——董事勤勉义务的具体化与内在化》，载《东南大学学报（哲学社会科学版）》2012年第5期，第76页。

〔49〕 参见王东光：《组织法视角下的公司合规：理论基础与制度阐释》，载《法治研究》2021年第6期。

必产生张力与冲突。〔50〕

客观分析上述观点学说都有其合理之处，内部控制并非一个法学概念，包括公司治理、风险管理和企业合规的各个流程，这决定了其行为本身可能属于广义信义义务其中的一种类型，需要将《个人信息保护法》第 58 条和信义义务的子义务做综合理解，利用忠实义务、诚信义务和勤勉义务拓展个人信息保护义务的实质内容。应该避免法律义务的“大词化”倾向，尽量提供一些充满血肉的制度安排。《公司法》修订过程中，部分学者建议将合规义务确立为公司和相关成员的基本义务，借此建构整个合规理论体系。〔51〕但是加入合规义务可能导致本就抽象的信义义务更加混乱，增加无谓的概念重叠与指向冲突。因此，本文不建议将内部控制行为作为一种新型合规义务，借由合规义务与信义义务并列的方式在《公司法》上确立下来。正如学者所说：“一个连注意义务都没有能力去具体界定的法律制度，如何去设定在此基础上更复杂的合规？”〔52〕

（五）职能设计和人员构成

在职能设计上，独立机构的监督职能体现为两方面：第一，监督职能本质上是督导并举而非狭义监督，应该扩充独立机构的实际职能。不同于外部监督事后纠错，独立机构的监督活动是对个人信息风险的内部控制活动，不仅局限于监控活动，而且包括控制环境、风险评估、控制活动、信息交流四个环节。第二，监督职能属于系统监督而非具体监督，应该减轻独立机构的职责负担。超大型平台企业规模巨大，包含各种业务类型，难以指望任职董事进行具体监督。“董事负有对公司作为一个运行良好的系统的‘设计者’和‘维护者’的职责，负有督导（monitor）的义务。”〔53〕系统监督与具体监督的不同，是划分独立机构与个人信息保护负责人工作职责的重要标准。

在人员构成上，专门委员会人员数量应保持单数，由三名或三名以上成员组成。可根据实际情况，由董事会提名委员会动态调整。独立董事应至少占全部人员三分之二及以上。其余三分之一，控股股东和负责个人信息保护的高级管理人员不得担任。为不干扰企业正常经营，在日常性管理中独立董事由超大型平台企业自行选任，平台企业应及时向主管部门备案公示。在合规整改时，为保证整改措施及时到位，可由主管部门指定独立董事人选。独立董事的任职条件，除了符合《上市公司独立董事规则》的各项要求外，还应该强调专业性与多样性。鼓励企业聘请具有一定个人信息保护专业知识的法律、计算机、企业管理等领域专家进入专门委员会。考虑到承担系统监督的工作职责，专门委员会成员理应从平台企业领取适当报酬。

（六）方案存在的弊端

决策监督型独立机构方案将独立机构设置在董事会内部，由独立董事具体履行监督职责，独立于董事经理等高级管理人员，具有一定的合理之处。同时也存在诸多弊端：第一，各种独立董事组成的专业委员会过多，容易造成董事会负担过重。机构人员臃肿效率低下。环境保护委员会、合规委员会、劳工权益委员会、可持续发展委员会、社会责任专门委员会等各种委员会都多

〔50〕 参见前引〔23〕，汪青松、宋朗文。

〔51〕 参见前引〔33〕，赵万一文。

〔52〕 邓峰：《公司合规的源流及中国的制度局限》，载《比较法研究》2020 年第 1 期，第 44 页。

〔53〕 邓峰：《领导责任的法律分析——基于董事注意义务的视角》，载《中国社会科学》2006 年第 3 期，第 143－144 页。

少已经存在，有些是法律强制规定的，有些是企业根据自身情况设立的，不同委员会之间存在职能重叠，很容易造成独立董事身兼多职负担过重。第二，独立董事平衡股东利益、利益相关者利益和公共利益，虽然理论上可以抽象证成，但实际操作存在困难。加之独立董事职能责任众多，很难周全各种利益诉求。第三，独立董事法律责任不明，容易挫伤独立董事的积极性。2021 年 11 月 12 日广州市中级人民法院判决康美药业五名独立董事因违反勤勉义务承担连带责任，合计赔偿金额最高约 3.69 亿元。此案引发了有关独立董事法律责任的争论。我国独立董事多为兼职担任，无论是信息来源、时间精力，还是对企业业务的了解程度，实际上都无法与公司董监高相比，在客观条件受限的情况下倡导提高独立董事法律责任存在一定问题。我国《公司法》欠缺对勤勉或注意义务的制度化建构，二者本身是一个不确定法律概念，内涵外延都有待明确。《个人信息保护法》虽然已颁布实施，但是为时尚短仍需实践，不少具体规则也仍在探索之中，极有可能造成权责畸轻畸重。

五、结语：合规监督的模式选择

根据上文分析可知，第三方独立机构方案欠缺独立性，不具有比较优势，无法承载《个人信息保护法》第 58 条第 1 项的功能期待，因此该方案应该被否定舍弃。管理监督型独立机构方案可以实现对经理层和业务部门的日常监督，但无法解决独立机构对谁负责的问题，由于难以介入董事会决策，始终面临企业合规动力不足的问题。决策监督型独立机构方案，虽然实现了对企业管理层的全面监督，但是容易发生利益冲突，日常情况下难以区分不同利益诉求，受制于法律义务规定模糊，容易承担过重的法律责任。由此可见，无论是管理监督型独立机构方案，还是决策监督型独立机构方案，都存在合理之处与固有弊端。能否通过制度安排扬长避短呢？超大型平台侵犯个人信息具有隐蔽性，宏观决策、中观执行和微观操作都需要进行有效合规和必要监督。两种监督方案都属于合规监督的具体类型，只能在各自的制度场景下合理运行，无法通过一种模式解决所有问题，需要明确两种方案所属的合规监督模式。

根据已有文献研究，管理监督型独立机构方案应属于“日常性合规管理模式”的具体展开，该模式是指“企业在没有违法、违规或者犯罪的情况下，根据常态化的合规风险评估结果，为防范企业潜在的合规风险，开展合规管理体系建设”〔54〕。这种合规监督模式关注日常管理和风险预防，独立机构主要监督业务部门实际运作和搭建完整合规体系，在企业没有出现重大安全风险和受到法律制裁时，只需对董事会负责即可，显然无需任何决定和认定都向主管部门报告。决策监督型独立机构方案应属于“危机性合规整改模式”，该模式是指“企业在面临行政执法调查、刑事追诉或者国际组织制裁的情况下，针对自身在经营模式、管理方式、决策机制等方面存在的漏洞和隐患，进行有针对性的制度修复和错误纠正”〔55〕。在此种模式下，该方案的问题可迎刃而解。为指导涉事企业有针对性进行合规整改，执法机构可选派政府工作人员或法律专家担任企业

〔54〕 陈瑞华：《有效合规管理的两种模式》，载《法制与社会发展》2022 年第 2 期，第 6 页。

〔55〕 前引〔54〕，陈瑞华文，第 6 页。

独立董事，此时仍处于危机应对阶段，因此各方利益诉求相对清晰，实现企业合规和恢复正常经营是多方主体的最大利益公约数。根据执法机构出具的合规整改意见，独立董事的监督义务明确，由此承担不合比例法律责任的情形很难出现。同时，独立机构的监督对象是整个企业管理层，外部监督直接介入企业运行，此时独立董事向主管部门汇报整改情况，在法律上也并不存在解释障碍。综上所述，管理监督型独立机构方案适用于日常性合规管理模式，决策监督型独立机构方案适用于危机性合规整改模式。在区分日常管理和危机应对两种合规监督场景下，两种方案的制度优势可以最大程度发挥，而制度劣势可以相对减弱。

Abstract: Paragraph 1 of Article 58 of the Personal Information Protection Law stipulates that super large platform enterprises should establish independent institutions mainly composed of external members to supervise the protection of personal information. At present, there are three system design schemes. The third-party independent institution scheme has no obvious comparative advantages, does not conform to the concept of risk prevention, and is difficult to carry the expectation of supervision function, so it should be abandoned. The plan of management and supervision independent institution belongs to the daily compliance management mode, which is the management supervision of the board of directors to the managers. The activities of independent institutions under the leadership of the board of directors can not solve the problem of compliance motivation, and it is difficult to clarify the tension between the board of directors and law enforcement agencies. The decision-making supervision type independent institution scheme belongs to the crisis compliance rectification mode, which is the rectification supervision of the law enforcement agency to the board of directors. A special committee of the board of directors is established to rely on independent directors for internal control. However, the legal responsibilities of independent directors are vague, which is easy to cause overburden on the board of directors. The two schemes have their own advantages and disadvantages, and should be applied separately according to the problem scenarios to realize the systematic and continuous protection of citizens' personal information.

Key Words: super large platform, independent institution, management supervision, decision supervision

(责任编辑：周　游　赵建蕊)