个人信息保护中的企业隐私政策及政府规制

高　秦　伟*

摘要：为充分保护个人信息安全，企业利用隐私政策的方式告知用户网站如何收集、处理个人信息，是否分享给第三方等内容，进而由用户选择是否继续从事网络行为。然而，由于企业隐私政策标识不明显、条款晦涩难懂，用户很少阅读；有时甚至存在欺诈和不正当竞争行为，导致其并未发挥应有作用。企业隐私政策是贯彻告知与选择机制的重要措施，兼具合同与规制工具特性。一方面，企业要发挥自我规制的功能，通过企业商业实践，不断完善隐私政策的实现机制，进而切实提升个人信息保护的水准；另一方面，政府须加强对企业隐私政策的规制，确保其具有可执行性。政府、企业和行业组织的合作规制将能更加充分地保障个人信息安全，个人信息保护立法应在合作规制上加大力度，并在学理上进一步加强体系化的思考，使各方主体真正发挥作用。

关键词：个人信息　　隐私政策　　告知与选择　　合作规制

一、问题的提出

当前全球个人信息保护的情况不容乐观。美国著名社交媒体脸书（face book）外泄个人信息的报道在全球引发热议，[①]我国支付宝年度账单引发的个人隐私争议也备受公众关注，相关企业先后被政府约谈。[②] 这涉及个人信息安全、企业隐私政策（privacy policy）及其政府规制的问题。事实上，从2017年下半年起，为推动互联网企业提高个人信息保护力度，提升行业个人信息保护的整体水准，由中央网络信息办公室、工业和信息化信部、公安部、国家标准化委员会等4部门组成的专家工作组对一些企业网络产品和服务的隐私政策展开了评审。[③] 为此，隐私政策也愈来愈受到互联网企业的重视，他们纷纷在其网站显著位置公布隐私政策，以便用户知情和同意。众所周知，网络与信息技术的发展给个人信息保护带来了严峻的挑战，如移动互联网可以随时随地收集和处理个人信息，云计算使个人信息远离了个人终端，社交网络使个人信息的公开成为用户自愿且日常化的行为，大数据分析可以轻易地将非个人信息转化为个人可识别信息，等等。企业隐私政策是用户了解企业个人信息处理活动的重要渠道，但据粗略估算，若要用户真正去阅读其访问网站的隐私政策，每年人均将花费约250小时，既耗时又不便。[④] 我国学者认为，企业隐私政策主要目的在于消除公众的顾虑，具有告知功能和制约功能。然而，从实践情况来看，两项功能均未

* 中山大学法学院教授、博士生导师

基金项目：国家社会科学基金项目（17@ZH014）

① 参见叶丹：《Facebook数据泄露敲响互联网信息安全警钟》，http://www.xinhuanet.com/zgjx/2018－03/23/c_137059108.htm，2018－03－26。

② 参见冯群星等：《支付宝年度账单引发隐私争议，为什么我们反而觉得是好事？》，http://news.163.com/18/0103/23/D78V8FTH000187VE.html，2018－01－05。

③ 评审范围包括隐私政策的内容、展示形态、用户同意等，参见《中央网信办等四部门联合开展隐私条款专项工作》，http://www.cac.gov.cn/2017－08/02/c_1121421829.htm，2017－08－05。2018年8月底，第2次隐私政策专项工作又正式启动，同时许多协会、消费者组织也展开了个人信息收集与隐私政策测评工作，提高了全社会层面对个人信息保护的关注度。参见王融：《迷雾中的新航向——2018年数据保护政策年度观察》，http://www.sohu.com/a/285519767_455313，2019－01－06。

④ 参见崔聪聪等：《个人信息保护法研究》，北京邮电大学出版社2015年版，第67页。

有效发挥作用。[①] 原因或许在于,企业隐私政策冗长且充斥大量的专业术语,用户并没有被充分告知,许多个人信息都是在用户不知不觉之间被企业共享或者出售给第三方主体;同时,企业隐私政策的性质也并不清晰,发生纠纷时难以约束企业。企业隐私政策究竟能够发挥多大作用,政府可否规制以及如何规制,目前的研究还不够深入。特别是在欧盟实施《通用数据保护条例》、美国加州议会通过《消费者隐私法案》的全球大背景下,中国的个人信息保护立法应当如何展开,企业和政府如何各司其职,均需要从学理上加以研讨。[②]

二、企业隐私政策的性质及实践

自个人信息保护法或者隐私保护法肇始,"告知与选择"(也称为告知与同意)一直是立法中最为重要和普适的机制。[③]"告知"是公开透明要求的体现,目的在于克服信息不对称而产生的市场失灵现象;而"选择"的内涵为同意,即用户在知情的前提下理性作出选择。《经济合作与发展组织隐私保护指导纲领》《亚太经济合作组织隐私保护纲领》、欧盟《数据保护指令》和《通用数据保护条例》、美国《公正信息实践原则》、我国《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》(2012 年 12 月 28 日第十一届全国人民代表大会常务委员会第三十次会议通过)和《中华人民共和国网络安全法》(以下简称《网络安全法》)等个人信息保护立法,均强调个人信息的收集、处理必须经过信息主体的同意。在这一机制之下,用户被企业告知产品服务信息及相关的隐私政策;进而,用户选择是否使用该在线产品或服务,并期望企业充分保障自己的个人信息或隐私安全。

(一)概念与形态

隐私政策是指互联网企业以在线文件的方式自愿披露其对用户个人信息保护的原则和措施。[④] 实践中,互联网企业一般都会在网站主页上公布自己的隐私政策,以确保告知与选择机制顺利实现。此种自愿性声明允许用户自主选择且对市场运作不予干预,业已成为世界多个国家和地区的通行作法。目前,我国绝大多数的互联网企业均在网站主页下端设有隐私政策方面的规定,如腾讯网、新浪微博的隐私政策主要包括企业如何收集、使用、分享转让个人信息,用户如何分享个人敏感信息以及如何确保信息安全等方面的内容。[⑤] 隐私政策通常按照产业发展规律或者行业自律标准而制定,目的在于保障用户个人信息的安全,同时也声明用户对于个人信息拥有的权利,包括被告知自己的信息被收集的权利、被告知个人信息在线提交的安全程度的权利、选择是否在线提交个人信息的权利、在线访问和修改自己的在线个人信息的权利、寻求纠纷解决的权利等。之所以利用这一机制,原因在于传统的政府规制多以命令控制型规制为主,实施过于严格、僵化,并存在阻碍创新与竞争的可能。[⑥] 同时,这一机制具有自愿性,不会对数据的合理流动造成不必要的限制,便于企业执行。面对多种多样的用户需求,市场与自愿性的解决方案或许能更有效地解决问题。总之,科学、规范的隐私政策能为企业提供竞争优势,吸引更多的用户注册、提高网站的访问率;而隐私政策不合理的企业则可能面临客户流失、利润下降的窘境。

企业隐私政策提升了网站运作的透明度,几乎所有的大型互联网企业均自发制定了隐私政策并加以

---

① 参见谈咏梅、钱小平:《我国网站隐私保护政策完善之建议》,《现代情报》2006 年第 1 期;京东法律研究院:《欧盟数据宪章——〈一般数据保护条例〉GDPR 评述及实务指引》,法律出版社 2018 年版,第 51～53 页。

② 第十三届全国人民代表大会常务委员会立法规划将《个人信息保护法》列为"条件比较成熟、任期内拟提请审议的法律草案"。《十三届全国人大常委会立法规划》,http://www.npc.gov.cn/npc/xinwen/2018－09/10/content_2061041.htm,2018－09－11。

③ See Daniel J. Solove, Introduction: Privacy Self－Management and the Consent Dilemma, 126 Harvard Law Review, 1880 (2013).

④ See Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Columbia Law Review, 583 (2014).

⑤ 参见腾讯网:《隐私政策》,http://www.qq.com/privacy.htm,2018－01－30;新浪微博:《微博个人信息保护政策(修订版)》,http://weibo.com/signup/v5/privacy, 2018－01－30。

⑥ See Jerry L. Mashaw, David L. Harfst, From Command and Control to Collaboration and Deference, 34 Yale Journal on Regulation, 167 (2017).

实施。此外,企业产品和服务还可以通过其他形式完成告知与选择功能,包括:[①](1)增强式告知,即注册账号、安装程序、首次使用时向用户展示的关于个人信息保护的提示。其并非传统意义上的隐私政策,而是对企业隐私政策核心内容的高度浓缩,即使用户之前没有阅读隐私政策,通过增强式告知也能够知晓隐私政策的核心内容,了解风险较高的个人信息处理行为。(2)即时提示,网站针对个人敏感信息处理行为,在用户使用互联网过程中即时展示相关的处理行为。[②] 用户通常都希望隐私政策中的相关内容能够真正得到应用和落实,而非停留于静态的文字。

(二)定性与学说

为回应广大用户对个人信息安全的关切,互联网企业将隐私政策与传统的合同性文本(如服务使用协议)相剥离而成为独立的文本或网页。其在定性上主要存在两种观点:

1. 合同说

国外学者一般认为企业隐私政策系网站和用户之间的合同。[③] 我国亦有持合同说者,认为"隐私政策的性质已经不再是一种声明,而是建立在双方合意基础上的协议,是网络服务合同不可缺少的一部分"。[④]还有人认为隐私政策是"网络格式合同",指出中国现行立法中虽无网络格式合同的概念,但满足"相对人有机会了解条款内容"和"明示同意"两个条件的网络格式合同应当得到法律承认,并适用格式合同的相关法律规定。[⑤] 司法实践中也基本上将用户协议和企业隐私政策视为性质相同的合同,进而适用合同法。如在"卢星与小米科技有限责任公司网络购物合同纠纷案"中,二审法院就将原告与被告之间的用户协议和企业隐私政策均视为合同。[⑥] 不过在实践中,一些国家的法院经常会针对不同的情形,作出具有差异性的判断。例如,在一起案件中,原告起诉美国航空公司违反企业隐私政策将乘客信息移交给联邦交通运输安全局,法院对违反企业隐私政策系违反合同的主张予以认可。[⑦] 而在另一起案件之中,法院对企业隐私政策的合同属性则持怀疑态度,认为如此宽泛的声明并不构成合同条款。[⑧]

这里的问题在于,网络上的同意方式一般分为点击生效和浏览生效两种。[⑨] 在点击生效的情况下,用户点击"我同意"或者"我接受"等按钮,即表示其在使用网站之前已经同意企业隐私政策的内容,因此网站和用户均会受到合同法的拘束。点击生效的协议易于确定用户是否以及何时同意协议的内容,具有较强的可执行性。而在浏览生效的情况下,则很难认定企业隐私政策具有拘束性。虽然从形式来看,用户如果不同意相关的协议就无法浏览网页,但事实上并无拘束力,故一些法院认为浏览生效并不构成同意。[⑩] 就企业本身而言,因为已存在服务使用协议,其也不愿将隐私政策视为合同,故主张企业隐私政策在性质上仅仅为政策声明,并不具有执行性。法院很少将隐私政策视为合同的另一个重要原因在于,原告较难证明其因企业违反义务而遭受损害。当然,法院或许可以适用"允诺禁反言原则",这一原则要求允诺人不得对已使受诺人产生信赖的诺言进行反悔,主要适用无过错归责原则。[⑪] 但在实践中,原告仍然面临举证难题,这使人们对告知与选择机制的有效性产生了疑虑。因此,合同法难以成为解决企业隐私政策争议的有

① 参见洪延青:《网络运营者隐私条款的多角色平衡和创新》,《中国信息安全》2017 年第 9 期。

② 关于个人敏感信息的区分,参见汤敏:《论同意在个人信息处理中的作用——基于个人敏感信息和个人一般信息二维视角》,《天府新论》2018 年第 2 期。

③ See Scott Killingsworth, Minding Your Own Business: Privacy Policies in Principle and in Practice, 7 Journal of Intellectual Property Law, 57 (1999).

④ 谈咏梅、钱小平:《我国网站隐私保护政策完善之建议》,《现代情报》2006 年第 1 期。

⑤ 参见贾旭凤:《从在线隐私政策看 B2C 电子商务中消费者个人信息保护规制》,硕士学位论文,华东政法大学,2007 年,第 18~19 页。

⑥ 参见甘肃省天水市中级人民法院(2016)甘 05 民终第 427 号民事判决书;"许斌与小米科技有限责任公司买卖合同纠纷案",杭州市中级人民法院(2016)浙 01 民辖终第 483 号民事判决书。

⑦ See In re American Airlines, Inc., Privacy Litigation, 370 F. Supp. 2d 552, 567 (N. D. Tex. 2005).

⑧ See Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1200 (D. N. D. 2004)(案件涉及航空公司非法共享乘客的个人信息).

⑨ See Deborah Davis Boykin, Survey of E-Contracting Cases: Browsewrap, Clickwrap, and Modified Clickwrap Agreements, 68 Business Lawyer (ABA), 257 (2012).

⑩ See Specht v. Netscape Communications Corp., 306 F. 3d 17, 32 (2d Cir. 2002).

⑪ 参见海静:《论英国法上的允诺禁反言原则》,《社会科学动态》2017 年第 2 期。

效工具。

2. 规制工具说

企业隐私政策是实施告知与选择机制的首要方式。有效告知意味着企业必须向用户公开收集、使用个人信息的相关作法;选择则是基于告知、同意而作出,既可以保障个人不同的信息偏好,又促进了数据合理流动。因而有学者将其视为一种企业自我规制的工具。[①] 在此框架下,在对产品、服务以及个人信息保护水准进行理性比较的基础上,用户自主决定个人信息是否被收集、利用和共享。企业通过隐私政策将自身的个人信息保护实践公诸于众,同时也为行政机关提供了规制依据,进而形成了企业自我规制和政府规制的互动。以美国为例,20 世纪 90 年代,因应公众对个人信息的关切,联邦贸易委员会成为个人信息与隐私保护的行政机关。[②] 它认为自己并无足够的能力制定实体性的隐私保护规则,僵化的政府规制还可能会抑制网络发展,于是在实践中鼓励企业自我规制,将执法限缩于对企业隐私政策的审查和规制。[③] 由此,企业自行创制保护个人信息和隐私的政策,并由行政机关监督规则的实施,就成为美国个人信息保护的主要作法。欧盟个人信息保护立法虽然极为强调政府规制,但自我规制也是其不可或缺的组成部分。[④] 当企业的自我规制失灵时,行政机关的监督和审查便作为"后盾",这不仅能够确保自我规制的合法性,而且使用户将企业隐私政策视为一种可信任的个人信息保护工具。

客观地讲,以上两种学说只是从不同视角展开的观察,前者围绕企业和用户的关系展开,后者则从行政机关和企业的关系层面进行描述,两者并无实质性冲突。问题在于,如何科学地认识企业隐私政策在政府规制中的作用。实践中,由于时间原因,用户很少阅读隐私政策;即使阅读,也常因为隐私政策充斥晦涩的法律术语望而却步。因此,用户往往因为微小的商业利益而低价出售自己的个人信息。[⑤] 企业出于商业利益的驱动往往忽视隐私政策的承诺,而行政机关又难以有效应对快速发展的网络和信息技术。[⑥] 诸如此类的问题导致个人信息和隐私保护面临巨大的挑战,使传统的私法保护或公法模式出现失灵。基于此,如何发挥私法和公法的共同作用,如何从政府规制视角来看待企业隐私政策的合同拘束效果,有待进一步探讨。

(三)实践与不足

在网络服务活动中,企业隐私政策会对用户产生显著的影响。隐私政策通过在企业和用户之间建立信任,切实促进了用户的信息披露意愿。[⑦] 不过,实践中企业隐私政策的实施也存在诸多不足,主要体现在以下几个层面:(1)由于隐私政策的内容用语通常较为宽泛、模糊,致使有些用户认为只要确认当前的隐私政策,网站就不会将其个人信息共享给第三方,但事实并非如此。企业违反对用户的承诺、不遵守隐私政策的情况时有发生。[⑧] 例如,未经用户同意收集个信息,在用户不知情的情况下安装软件收集个人信息;非法搜集用户个人信息形成画像,用于定向推送商业广告等目的;将个人信息非法转售给第三方,甚至

---

① See Joel R. Reidenberg et al., Privacy Harms and the Effectiveness of the Notice and Choice Framework, 11 I/S: Journal of Law and Policy for the Information Society, 485 (2015).

② See Steven Hetcher, The De Facto Federal Privacy Commission, 19 John Marshall Journal Computer and Information Law, 109 (2000).

③ See FTC, Self-regulation and Privacy Online: A Report to Congress, https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf, 1999, pp.12-14, 2017-12-12。

④ 参见欧盟《数据保护指令》第 27 条、《通用数据保护条例》第 40 条的规定。国内相关讨论可参见周汉华:《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》,《法学研究》2018 年第 2 期。

⑤ See James P. Nehf, Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy, University of Illinois Journal of Law, Technology & Policy, 1 (2005).

⑥ See Nadezhda Purtova, The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law, 10 Law, Innovation and Technology, 40 (2018).

⑦ 参见刘百灵等:《网络环境下基于隐私政策的隐私保护研究综述》,《情报理论与实践》2016 年第 9 期。

⑧ See J. R. Reidenberg et al., Disagreeable Privacy Policies: Mismatches Between Meaning and User's Understanding, 30 Berkeley Technology Law Journal, 39 (2015).

破产时将个人信息出售用以抵债,等等。[①] (2)由于企业隐私政策的内容专业且冗长,对于不具备充分法律知识的用户而言,即使全面阅读也徒劳无益。(3)由于企业自身能力的不足,隐私政策很难准确地说明以及预测个人信息处理和利用的情形。(4)互联网企业经常单方面改变隐私政策,而未将相关修改事先告知用户。(5)随着大数据技术的发展,信息整合将披露更多的个人敏感信息,而用户无法理解未来信息整合的影响,也无法评估未来可能带来的损害,从而很少认真阅读企业隐私政策;即使事后发现个人信息或隐私受到侵害,也往往因难以证明损害事实而败诉。这使得隐私政策常常成为企业逃避责任的挡箭牌。

实践中,企业隐私政策个人信息保护效果常因企业能力、重视程度等因素而呈现出较大的差异,对个人信息安全产生了巨大的影响,因此用户不断要求政府予以规制。如即使是主张隐私自我规制的美国,也有法案提出以政府规制全面替代企业的自我规制。[②] 不过,这些立法提案并没有得到美国国会的认可。原因在于企业隐私政策虽然存在不足,但是一方面完全依赖于政府规制则会抑制企业创新,企业唯有真正重视隐私政策及其实施过程,自我规制方可发挥作用;另一方面企业隐私政策本身可以成为执法依据而被行政机关强制执行。尤其是后者,往往被各国在推行企业隐私政策之时所忽略。[③]

三、内部修正:告知与选择机制的存废和改进

从国内外个人信息保护立法来看,告知与选择机制业已成为个人信息保护的主要趋势,并在个人信息保护实践中获得普遍认可。在具体操作中,互联网企业通过制定隐私政策并采取相关技术措施来贯彻告知义务和保障信息主体的选择权。由于每个人的隐私倾向不尽相同,告知与选择机制的灵活性可以避免武断地为个人信息保护设置整齐划一的标准,从而利用用户自治避免过度规制引发的僵化后果。然而,从前述分析来看,此种机制在个人信息保护方面存在一定的缺陷。尤其是大数据背景下,个人信息不仅是私人物品,而且具有不容忽视的社会公共属性,业已成为互联网产业发展的主要动力。此时,用户个人的同意可能很难承载这种公共意志。同时,需要企业在隐私政策中告知什么内容亦面临较大的挑战,因为在大数据时代,收集什么信息、如何使用信息、结果如何等,均可能处于不确定的状态。[④] 在企业、用户均无法充分理解面临的情形时,对个人信息与隐私的全面保护便可能成为奢望。那么,告知与选择机制的出路何在?如何使企业隐私政策更加有效?本部分将主要从企业内部视角加以探讨。

(一)告知与选择机制的存废

由于告知与选择机制在实践中运行不甚理想,包括企业隐私政策在内的相关设计是否有必要继续存在,成为近年来个人信息保护立法的一个热点议题。对此,肯定说认为:对于网络发展及其产生的问题,传统的命令控制型规制很难发挥作用,而要求企业披露相关内容远比对个人信息保护问题作出实体性规制容易。虽然告知与选择机制存在问题,但在实现个人自主选择权方面仍有不可替代的作用,其可以避免政府直接介入带来的不良后果。将个人信息保护的任务交由企业,可以充分满足不同用户、不同产业、不同商业模式的差异化需求,可以促进科技创新和电子商务的快速发展。基于信息披露的规制工具自身并不能解决所有问题,不可片面强调告知与选择机制的局限。以环境保护领域为例,信息披露之后尚需其他规制工具配合才能实现环境治理的目标。[⑤] 虽然告知与选择机制、企业隐私政策的适用效果不尽如人意,但并不代表它不重要,更不能否定其存在的必要性和正当性,应要进一步明确该机制和企业隐私政策的适用范围与形式,并对处理个人信息的全过程予以监督。[⑥] 否定说认为:首先,在告知与选择机制下,企业所提

① See Brian Carroll, Price of Privacy: Selling Consumer Databases in Bankruptcy, 16 Journal of Interactive Marketing, 47 (2002).

② See Richard Warner, Surveillance and the Self: Privacy, Identity, and Technology, 54 DePaul Law Review, 847 (2005).

③ 参见个人信息保护课题组:《个人信息保护国际比较研究》,中国金融出版社 2017 年版,第 113~114 页。

④ See Julie E. Cohen, The Regulatory State in the Information Age, 17 Theoretical Inquiries In Law, 369 (2016).

⑤ See Ronan Kennedy, Rethinking Reflexive Law for the Information Age: Hybrid and Flexible Regulation by Disclosure, 7 George Washington Journal of Energy and Environmental Law, 124 (2016).

⑥ 参见徐丽枝:《个人信息处理中同意原则适用的困境与破解思路》,《图书情报知识》2017 年第 1 期。

供的是要么全盘接受要么悉数拒绝的条款，作为个体的用户并不具备与网站协商隐私保护政策的谈判能力。[①] 多数情形之下，隐私政策成为企业逃避责任的工具，告知与选择机制难以成为个人信息处理的正当性基础。其次，告知与选择机制片面强调个人知情同意的重要性，而忽视了个人信息的社会属性及其作用。[②] 目前的立法和实践赋予企业更多的裁量权，鼓励企业以功利的目的收集个人信息并从中获利，而对个人信息的社会作用及其实现关注不够。有必要将个人信息保护从程序规范保护机制转向实体规范保护机制，在企业、用户之间真正建立充分的信任关系。[③] 最后，告知与选择机制仅关注个人信息收集的初始阶段，事实上，使用、交易等信息处理环节也同等重要，相关行为是否需要经过信息主体的再次同意，由哪个组织来监督等，均值得深入讨论。

应该讲，以上两种观点均有一定的道理。在当前的技术背景下，有关个人信息保护的认知和实践发生了很大变化。大数据分析可能会挖掘出许多原本并非属于个人信息但却能清晰地识别出特定个人的信息，个人信息的用途也变得更难预测，这使得隐私政策无法详尽说明企业的个人信息保护实践。而在现实中，面对新技术，用户很难理解数据聚集产生的效应，也很难评估信息泄露、融合的潜在危害，更无法进行长期的成本收益分析，告知与选择机制似乎成了摆设。与此同时，个人信息的作用不仅对个人发展极为重要，对于社会发展也十分关键，其具有一定的公共性而成为当前信息产业的基础和支撑。[④] 因此传统的个人权利和信息正当使用的相关原则受到挑战，对于个人信息的公共物品特征也越来越得到强调。在新的技术发展背景之下，传统告知与选择机制必然受到冲击。然而，完全予以放弃则会因个人信息收集的“入口”过于宽松而带来更多问题。对此，可行的方案在于采取渐进措施改进该机制的不足。不过也应注意，透明度或者公开并非是信息正当利用的充分条件，尚需要与其他机制相结合。

（二）告知与选择机制的改进

作为告知与选择机制中最为重要的措施，企业隐私政策虽然在实际运行过程中存在诸多问题，但是从世界各个国家和地区的立法实践来看，并没有出现放弃该机制的迹象。这是因为，面对网络和信息技术的发展，政府直接介入可能产生抑制创新和竞争的不利后果，而发挥企业自我规制并对其进行适当监督，不仅可以促进创新，也有利于产业发展和个人信息保护。并非所有社会问题都可以通过行政手段解决，信息时代的社会问题更宜通过自下而上、自发学习和弹性合作的方式加以回应。为此，有必要从以下两个层面对企业隐私政策加以改进：

1. 侧重于企业隐私政策本身的改进

有学者认为，为使告知与选择的机制切实有效，要求隐私政策必须能够将企业的个人信息保护制度全面、准确地传达给用户，从而让用户作出理性的选择。为此，企业必须给用户提供内容明确、易于理解的信息。当然，作为用户，也应该认真阅读隐私政策。例如，2012 年美国联邦贸易委员会向国会提交的一份报告中就要求企业隐私政策必须明确、显著，不能使用相互矛盾的语言，并建议企业在隐私政策之前制作一个简明的摘要，此举被称为“分层告知”方式。[⑤] 分层告知是指将企业隐私政策的内容以表格或者其他标准化的方式加以公布，其意义在于为用户提供更为简明的告知方式以便阅读——惊鸿一瞥总比一无所知要好。实践亦证明，用户更愿意阅读以形象化方式公布的企业隐私政策。还有学者建议应该利用其他学

① See Kate Crawford & Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55 Boston College Law Review, 93 (2014).

② See Priscilla M. Regan, Legislating Privacy: Technology, Social Values, and Public Policy, The University of North Carolina Press, 2009; James P. Nehf, Recognizing the Societal Value in Information Privacy, 78 Washington Law Review, 1 (2003).

③ See Neil Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law, 19 Stanford Technology Law Review, 431 (2016).

④ See Joshua A. T. Fairfield & Christoph Engel, Privacy as a Public Good, 65 Duke Law Journal, 385 (2015); see also Dennis D. Hirsch, Privacy, Public Goods, and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel, 65 Duke Law Journal Online, 67 (2016); Priscilla M. Regan, Response to Privacy as a Public Good, 65 Duke Law Journal Online, 51 (2016).

⑤ See Corey A. Ciocchetti, The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices, 26 John Marshall Journal of Computer and Information Law, 1 (2008).

科的知识来促成更为有效的告知,以便让用户积极阅读并理解企业隐私政策,[①]如有人建议将食品安全、环境规制等领域的作法引入个人信息保护实践之中。[②] 当然,简化并不意味着用户无需阅读企业隐私政策的各项术语,而是要求企业不断改进隐私政策及其实现措施,以更为明确的方式让用户了解企业有关信息收集、使用和处理的制度。为了提升用户参与企业隐私政策制定和执行的能力,有建议强调应该通过公共教育促进对个人信息保护的重视;强调多元主体参与,建立网络隐私指引和认证机制、企业隐私政策协商制度等。[③]

2. 基于技术的解决方案

此类方案认为,对于个人信息保护的各项规则(包括企业隐私政策)均过于侧重程序性保护,忽视了实体性问题。实体性问题是指在强调个人信息主体知情同意时,对最少必要、目的明确、安全利用等规则也要以明确、易懂和合理的方式加以确定。基于技术的解决方案强调关注用户对个人信息和隐私安全的期望,并超越企业隐私政策本身而关注网站、软件和设备的整体结构与设计,制定更容易操作的同意规范、实践以及标准,也许这正是互联网规制机关、企业、行业组织等多方主体未来所要解决的重要议题。[④]

目前,"隐私增强技术"被视为基于技术的解决方案中较具代表性的做法,意在将实体性的隐私保护融入企业运作之中,且对企业产品和服务的整个生命周期予以关注,以实现全面保护个人信息安全的目的。隐私增强技术主要解决隐私和个人信息安全的单方面问题,以匿名化为例,通过对个人信息的技术处理,使得个人信息主体无法被识别,其是一种对产品或服务的后期设计与考量。再如万维网联盟为保护在线隐私发展出"隐私偏好平台"标准,该标准能够将用户浏览的网站的隐私政策与用户隐私偏好进行比对。[⑤]这一标准后来被一些企业所借鉴,不过结果并不理想。因为其作用仅仅在于增强企业隐私政策的透明性,使用户可以清楚地理解个人的何种信息被收集、用于何种目的以及存储多长时间,标准本身并不能保障网站履行其隐私政策,因而无法完全解决个人信息保护的根本问题。

基于技术解决方案的另一个代表性做法为"通过设计保护隐私"。目前经济合作与发展组织、欧盟、美国等均在立法中对信息管理者施加了通过设计保护隐私的义务,要求其在信息生命周期的最开始就去思考个人信息和隐私保护的问题,而不是在事件发生之后。[⑥] 此种机制的主要做法是将个人信息保护嵌入技术、商业准则和物理存在的基础设施的设计标准中并加以保护。信息管理者在设计产品或服务时,要将个人信息与隐私保护机制和业务结构、规模、数量和敏感度等因素予以关联。此种风险预防、技术与法律互动的思路克服了过去仅在信息收集时单纯依赖告知与选择机制的不足,让信息管理者甚至信息主体参与到企业运作和个人信息保护的全过程,有利于提升企业个人信息保护的能力和主动性。通过设计保护隐私主要针对整个系统,和隐私增强技术有一定的差异,但两者也经常会同时被使用。

从以上两个层面的改进方案来看,前者侧重于隐私政策本身的修正,而后者侧重于技术方面的改进。虽然技术性的解决方案未必是法学关注的重点议题,但是科技发展和法律规范形成之间的互动却值得关注,或许这种互动会为构建个人信息保护的实体性规范作出贡献。[⑦] 如依据技术分析和参数要求,可以确定特定行业在个人信息收集时最少必要原则的范围。同时,也可以看出,两种改进方案均处于不断完善和

① See Ryan Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87 Notre Dame Law Review, 1027 (2012).

② See A. Michael Froomkin, Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements, 2015 University of Illinois Law Review, 1713 (2015); Dennis D. Hirsch, Going Dutch: Collaborative Dutch Privacy Regulation and the Lessons it Holds for U. S. Privacy Law, 2013 Michigan State Law Review, 83 (2014).

③ 参见申琦:《我国网站隐私保护政策研究——基于 49 家网站的内容分析》,《新闻大学》2015 年第 4 期。

④ See Ira S. Rubinstein, Regulating Privacy by Design, 26 Berkeley Technology Law Journal, 1409 (2011).

⑤ See William McGeveran, Note, Programmed Privacy Promises: P3P and Web Privacy Law, 76 New York University Law Review, 1812 (2001).

⑥ See Stuart L. Pardau & Blake Edwards, The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity, 12 Journal of Business and Technology Law, 227 (2017).

⑦ See Helen Nissenbaum, Privacy in Context: Technology, Policy and the Integrity of Social Life, Stanford Law Books, 2009, pp. 158—159; Kenneth A. Bamberger, Deirdre K. Mulligan, Privacy on the Ground: Driving Corporate Behavior in the United States and Europe, The MIT Press, 2015, pp. 24—25.

发展之中，需要技术、法律、社会规范等方面共同协作，才会有更佳的效果。当然，因应现实中技术和商业模式的快速变迁，法律如何能够发挥自身的积极引导作用，亦将成为个人信息保护法治实践中的重要课题。

（三）我国的探索

《网络安全法》第41条关于用户告知同意的规则要求网络经营者收集、使用个人信息，应当遵循“合法、正当、必要原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。”但对于什么构成“正当、必要”以及企业告知和用户选择的具体方式，立法并未作出具体要求。实践中，使用企业隐私政策无疑是最符合成本收益的方式，企业对之趋之若鹜。随着用户权利意识不断增强，企业应当逐步确立“通过设计保护隐私”的理念，将个人信息保护的概念融入产品和服务中，而不能完全依赖隐私政策。但是，个人信息种类的多样性和信息利用方式的复杂性使针对个体用户提供定制化的产品或服务难以实现。再者，由于我国个人信息保护经验积累不多，也使告知与选择机制、企业隐私政策仍然是现阶段个人信息保护的主要举措。因此，中央4部门才会展开评估活动并将企业隐私政策视为个人信息保护的突破口。放眼未来，还需对企业隐私政策、告知与选择机制进行不断改进，细化相关立法规定，以为网络运营者和用户提供明确指引。

实践中，一些企业为了使个人信息安全保护更具针对性，根据个人信息收集和使用的必要性不同，将网络产品与服务的功能区分为核心业务功能和附加业务功能。核心功能旨在满足用户注册产品或服务后的基本要求，附加功能则是为提升用户体验而设计。以《京东隐私政策》为例，其第1条第1项明确告知用户产品或者服务的所有核心功能与附加功能，以及其收集个人信息的内容、目的和用途，并于第1条第2项明确告知用户拒绝提供或拒绝同意的后果。拒绝核心功能收集和使用个人信息的影响将是无法注册成为网络或产品的用户，并无法享受所有服务；拒绝附加功能收集和使用个人信息，则不会影响用户正常使用产品或服务的核心功能。[①] 也就是说，只有用户主动使用产品或服务的附加功能，且使用该功能须收集和使用用户个人信息时，才会触发通过设计保护隐私的“开关”，其相对于核心功能保护要求更加严格。与此同时，网络运营者仍然可在用户首次使用或注册时与用户签订统一的隐私政策，完成用户使用产品或服务的核心功能时收集和使用个人信息的授权。附加功能的使用有时还需要用户主动触发，例如主动点击同意或填写相关的个人信息。此种做法也被2018年起实施的国家标准《信息安全技术 个人信息安全规范》（GB/T 35273－2017）所吸纳。总体而言，我国的探索有一定的积极意义，但因个人信息保护缺乏整体性思路，加之这些自我规制机制多取决于企业自身的关注程度和实施意愿，故运用必要的政府规制加以监督才能使其真正发挥作用。

四、外部规制：企业隐私政策的效力实现与学理反思

面对个人信息不断被侵犯的情形和公众对隐私安全的高度关切，我国政府开始推动相关的立法及其实施工作。中央4部门之所以首先选择将企业隐私政策评估作为提升个信息保护的重要举措，原因在于：作为“入口”，企业对个人信息收集、处理和利用的无序化现象较为严重，隐私政策并没有很好地拘束企业行为，所以政府有必要予以干预。《网络安全法》要求企业重视隐私政策且政府应对之进行监督，但实践中，行政机关并未真正发挥应有的作用，导致许多企业的隐私政策徒有其表而不具有实际的可执行性和效力。因此在我国，要求互联网企业颁行隐私政策并对其作出评审只是第一步。从域外经验来看，要使企业隐私政策真正发挥作用，政府规制不可或缺。需要指出的是，与告知选择机制改进侧重企业隐私政策本身的完善不同，政府规制更加强调外部的处罚和监督，意在使企业隐私政策真正产生拘束效果。当然，这两个层面的内容也有所关联，旨在实现多元主体保障个人信息安全的状态。

（一）对企业自我规制的政府规制

① 参见《京东隐私政策》，https://about.jd.com/privacy/，2018－01－31。

互联网企业制定隐私政策是其应对个人信息保护立法的重要方式之一。例如,2018 年 5 月 25 日,谷歌公司在全球范围内同时发布了多语种的最新版隐私政策,以应对当日正式生效实施的欧盟《通用数据保护条例》。之所以如此,是因为该条例对企业的告知与选择机制进行了重点规范,要求企业个人信息保护必须贯彻合法、公平、透明原则,目的限定原则,最小范围原则,准确性原则、存储限制原则,完整性与保密性原则以及责任原则。这些原则均为概括性的规定,谷歌公司为改变过去对个人信息保护不利的负面形象,通过隐私政策进一步细化了这些规定。如在目的限定原则方面,旧版隐私政策并未特别说明为什么要收集信息,而只是较为笼统地说企业会利用从所有收集到的信息来提供、维护、保护和完善这些服务,同时开发新的服务并保护企业用户。新版隐私政策则用约两页的篇幅来解释企业为何收集信息,力求将收集个人信息的目的"具体、明确"地告知用户,并承诺将用户信息用于企业隐私政策未涵盖的用途时事先征求用户同意,以满足目的限制的要求。同时,随着隐私政策与互联网企业产品、服务、场景的结合越发紧密,企业隐私政策的实施水平与企业自我规制能力也密切关联。然而,鉴于谷歌、脸书等大型互联网企业个人信息泄露情况仍然较为严重,不可过分高估企业自我规制的作用。① 因此,为克服企业自我规制的不足,相关立法均规定了一定的政府规制措施,并以高额罚款作为保障。

以美国为例,根据《联邦贸易委员会法》的规定,联邦贸易委员会负责保护消费者利益并促进竞争。② 在互联网贸易领域,该法主要实行自我规制模式,但也依赖法定权力展开执法,切实保护用户隐私。该法第 5 节规定:"商业中或影响商业不公平的竞争方法,是非法的;商业中或影响商业不公平或欺骗性的行为及惯例,是非法的。" ③联邦贸易委员会通过执法解释了"不公平"和"欺骗性"的商业行为,相关的隐私保护执法行为逐年增加。联邦贸易委员会的执法活动从非正式调查开始,审查相关的信息或直接联系企业。如果认为必要,它还会向企业发出正式函件,要求提供文件和信息,进行约谈或要求作证,并可能访谈第三方。当联邦贸易委员会有充分理由认为存在违法情形,并认为诉讼程序符合公共利益时,就会提起指控。指控可通过两种途径解决:一是通过同意令来寻求违法方的主动合作。二是司法判决。同意令是双方通过和解协议解决争端,条件是企业明确同意服从联邦贸易委员会持续性的规制。规制以监督和审计为主,督促企业积极采取加强个人信息或隐私保护的措施。同意令仅服务于和解目的,不构成对违法的确认;其内容将被公开,并对企业今后的行为产生法律拘束效力,违反将被处以相当数额的罚款。实践中绝大多数的执法行为最终都以同意令的方式结案,其内容被企业视为个人信息保护的规范指南而加以执行。在批准同意令时,除遵守公开等程序性要求之外,一般还应考量如下实体性要求:(1)对错误行为的禁止;(2)罚款的同时要求企业承诺对用户予以赔偿;(3)告知用户及时采取相应的补救措施;(4)删除或限制使用相关信息;(5)要求企业对隐私政策作出调整和完善;(6)建立综合性的安全、隐私和信息整合体系。(7)由独立的专业机构展开进一步评估;(8)企业要履行记录保存和合规报告的义务,以便行政机关对同意令的实施情况进行检查;(9)企业对影响合规问题的重大变化要对外通告。④

再以欧盟为例,欧盟及其成员国虽然强调对个人信息进行严格保护、统一立法和政府规制,但实际上与美国殊途同归。⑤ 其赋予企业较多的合规裁量权,尽量减少使用命令控制型规制;同时,又以政府规制特别是正式的执行行为作后盾,有效地保护个人信息安全。⑥ 欧盟法要求各成员国应当将产业行为规范整合进各自的个人信息保护立法中,从而确保这些法律规范得到妥当的实施。各行业的行为规范应结合

① 参见刘绍宇:《论互联网分享经济的合作规制模式》,《华东政法大学学报》2018 年第 3 期。

② See Chris Jay Hoofnagle, Federal Trade Commission Privacy Law and Policy, Cambridge University Press, 2016, pp. 3—81.

③ 15 U.S.C. § 45(a) (1).

④ See Daniel J. Solove, Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Columbia Law Review, 583 (2014).

⑤ 为研究方便,这里暂且忽略欧盟和美国对个人信息或者隐私的认知及其相关保护模式之间的差异。See James Q. Whitman, The Two Western Cultures of Privacy: Dignity versus Liberty, 113 Yale Law Journal, 1151 (2004).

⑥ See William McGeveran, Friending the Privacy Regulators, 58 Arizona Law Review, 959 (2016); Dennis D. Hirsch, The Law and Policy of Online Privacy: Regulation, Self—Regulation, or Co—Regulation, 34 Seattle University Law Review, 439 (2011).

行业特点，各成员国政府会对这些规范进行审查，在确保规范内容与法律一致的情况下，行政机关还会征求信息主体和其他利害关系人的意见。典型如欧洲互联网企业最为集中的国家爱尔兰，虽然其规制机关拥有罚款等执法权力，但在实施过程中仍然十分注重企业自我规制，要求企业提升隐私政策告知的透明度和拘束力；行政机关与企业展开合作性规制，取得了良好的效果。①

综观各国，美国虽然一再强调个人信息保护以自我规制为主要形态，但政府规制也发挥了巨大的作用，进而形成了多元主体合作的状态；同样，企业自我规制与政府规制的结合，也正在成为欧盟及其成员国个人信息保护法的主要做法。② 政府规制的意义在于确保企业隐私政策的效力，同时，由于个人信息侵权案件举证困难，政府的介入可以弥补个体用户举证能力的不足；③此外，政府采取调查、评估等行为，将会企业经营形成声誉压力，从而迫使企业尽快采取和解行动并切实改正违法行为。需要指出的是，美国联邦贸易委员会在企业违反和解协议时而也会行使处罚权，且罚款数额必须反映出用户的损失。不过，执法行为可以不局限于企业违反隐私政策的行为，企业处理用户个人信息的安全措施均属于其调查权范畴之内。④ 例如，在一个和解案件中，联邦贸易委员会认为企业违反了确保用户个人信息保密的承诺，责令其改正；同时指出企业未能提供有关保护用户个人敏感信息的有效的培训、检查与控制机制。⑤ 相比之下，我国网络安全机关的法定权力更为广泛，应当充分利用并对企业隐私政策展开合理规制，全面保障用户的个人信息安全。

（二）学理反思：合作规制的思路及其未来课题

近些年来，个人信息保护问题受到各界的高度关注。虽然我国目前尚无统一的个人信息保护法，但相关法律规范已经分散存在于各种单行法中。有关企业对个人信息的收集、使用、共享等内容，我国亦采用与国外类似的做法，以告知与选择机制为主，注重企业自我规制。然而，随着个人信息泄露事件的大量发生，这种片面强调企业隐私政策而忽视政府规制的模式受到质疑。《网络安全法》实施以来，企业有关个人信息的运作缺乏惩罚机制、透明度不高、执行不力等现实问题让人们不得不重新审视政府规制介入的必要性。事实上，企业的自我规制和政府规制并非互相排斥，即使是崇尚自由市场主义的美国和以严格保护而著称的欧盟，也非单纯依靠自我规制或政府规制的方式来实现保护个人信息的目的。为了克服个人信息保护分散立法的不足，美国国会一直试图就隐私保护展开立法，联邦贸易委员会也在积极实施规制行为，对企业自我规制予以再规制。就我国而言，即使在未来实现个人信息保护统一立法，企业自我规制的配合作用也不可或缺，这一点已被欧盟及其成员国的立法与实践所证明。因此企业应当积极完善隐私政策及其实现方式，行政机关在必要时也应赋予企业隐私政策拘束力，督促企业切实保障个人信息的安全。

现代规制理论主张，在充分发挥市场机制和企业自我规制作用的前提下，政府规制也不能缺位。与以往放松政府规制而仅仅强调市场和企业自我规制不同，现代规制理论更加强调为企业和政府的合作提供规范和框架，未来，合作规制应该成为应对经济社会问题的重要思路和措施。⑥ 政府规制依据详细的规则展开适用并得以发现、惩罚违法行为，其虽然在某些领域效果理想，但也存在成本高、效率低和过度干预市场的弊端。在一般情况下，政府规制对市场情况不作区分而采取“一刀切”的僵化措施，难以与行业保持同

① See Data Prot. Comm'r, Report of Audit: Facebook Ireland Ltd. 3 (Dec. 21, 2011), http://www.dataprotection.ie/docs/Facebook－Ireland－Audit－Report－December－2011/1187.htm, 2018－01－02。

② See Francesca Bignami, Cooperative Legalism and the Non－Americanization of European Regulatory Styles: The Case of Data Privacy, 59 American Journal of Comparative Law, 411 (2011).

③ 个人信息侵权的举证问题一直困扰司法界，政府介入无疑会给企业形成压力，有利于用户维护合法权益。我国法院有关个人信息侵权案件举证责任分配存在的争议可参见“庞理鹏与北京趣拿信息技术有限公司等隐私权纠纷案”，北京市第一中级人民法院(2017)京01民终509号民事判决书；“林念平与四川航空股份有限公司侵权责任纠纷案”，成都市中级人民法院(2015)成民终字第1634号民事判决书。

④ See Joel R. Reidenberg et al., Privacy Harms and the Effectiveness of the Notice and Choice Framework, 11 I/S: A Journal of Law and Policy for the Information Society, 485 (2015).

⑤ See Complaint, In re Eli Lily & Co., FTC File No. 012 3214, No. C－4047 (F.T.C. May 8, 2002).

⑥ See Ira S. Rubinstein, Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes, 6 I/S: A Journal of Law and Policy for the Information Society, 355 (2011); Margot Priest, The Privatization of Regulation: Five Modes of Self－Regulation, 29 Ottawa Law Review, 233 (1998).

步发展,从而阻碍创新。与此相对,企业自我规制虽然具灵活性、低成本、高合规率等优势,但缺乏责任、透明等机制保障。因此,如何使政府规制与自我规制有效结合,成为现代规制理论的核心议题。

合作规制整合了政府规制和自我规制的积极要素。在一般情形下,规制目标由政府设置,而如何实现及其方式则由企业自行确定,政府负责监督执行。有时政府会与企业达成协议共同来解决问题,有时则会涉及行业协会、非政府组织等主体的参与,从多个方面促进行政任务的实现。展开合作规制时应当注意:首先,合作而非对抗,要利用多种手段激励企业自我规制的意愿。合作规制现象在其他领域并不鲜见,但个人信息保护领域科技日新月异,需要企业践行更多的合作、履行更多的社会责任。① 其次,合作规制依赖企业或者协会等组织来行使政府的某些传统职能,弥补政府规制的不足。这使得合作规制的规则较传统立法更为开放,仅规定所欲实现的目标即可,从而赋予参与方充分的自主权。再次,由于企业和协会组织积极参与规则形成,使自我规制意愿和合规率得到极大提升。现代规制理论特别强调政府与企业等多元主体的合作,并对合作规制与自我规制加以区分,其意不仅在于指出政府介入程度的差异,更在于说明规范制定、责任分配、制裁方式、公众参与等方面的差异,②进而共同发挥政府、企业以及行业协会等多元主体各自的优势。③ 长期以来,我国的立法和实践普遍将政府规制、自我规制截然分开,要么放任企业恣意活动,要么由政府直接干预,突出两者的对抗而忽略了合作的内涵,强调规制结果而忽略了规制的过程,导致规制效果不尽人意。对此,必须予以反思。

一项规制的实现过程大体包括 3 个阶段:创立规则、合规监督(主要以日常监督为主)与规制实施(如处罚、吊销许可证)。在传统行政法上,这 3 个阶段主要由行政机关主导;而在合作规制中,各方主体均在不同程度上参与这 3 个阶段,从而使合作规制的形态呈现出多样化的特点。例如,自愿性的产业行为规范,虽然纯粹由企业或者行业协会制定、执行,但是政府也会出于公共利益的理由予以一定程度的介入。而在法定的自我规制项目中,企业、行业协会、政府则会共享前述 3 个阶段的权责,有时政府还会将合规监督的权力授予其他社会组织。④ 从理论上讲,合作规制给行政法带来的变化主要体现为 3 个层面:⑤

1. 规制主体多元化。面对个人信息保护日益严格的趋势,无论有无法律要求,企业均应以自我规制的方式对个人信息展开保护,而这些自我规制措施并非完全没有拘束力。在一定情况下,行政机关会进一步审查并给予相关的意见和建议。在实施过程中,除企业自我监督外,政府亦将发挥监督功能,行业协会、认证机构也会参与到规制实施的过程中来。在个人信息保护实践中,由个人信息保护组织或机构展开的个人隐私保护认证亦是一种成功的保护方法,有助于提升用户对企业个人信息运作的信任和信心。⑥

2. 规范结构的原则化。由于立法赋予企业、行业协会等多元主体参与规制的权利,合作规制结构下的法律规范呈现出框架立法的特征,这与立法尽量完整、详尽进而界定行为构成要件和法律责任的传统做法有所不同。法律规范将以原则性条款对规制目标、各方权限和责任、程序等加以规定,同时赋予行政机关进一步细化法律的权力。此种变化,使人们认识到并不是设定规范就足以实现规制目标。就政府而言,还须通过设定相应的政策决定程序、适当的行为形式、组织形态等,方可完成规制任务。就私人主体而言,企业的隐私政策、企业和规制机关签订的行政协议、声誉机制、第三方审核机制等均应发挥作用,才能切实保护个人信息和隐私安全。

3. 规制方式的多元化。除使用企业自我规制、传统命令控制型规制之外,合作规制的方式呈现出多元化的形态,诸如建议、和解、约谈、协商、推荐性标准、第三方规制等均得到广泛应用,且与私人规制和传统

① 参见张青波:《自我规制的规制——应对科技风险的法理与法制》,《华东政法大学学报》2018 年第 1 期。

② See Ira S. Rubinstein, Privacy and Regulatory Innovation: Moving beyond Voluntary Codes, 6 I/S: A Journal of Law and Policy for the Information Society, 355 (2011).

③ See Darren Sinclair, Self-Regulation versus Command and Control: Beyond False Dichotomies, 19 Law and Policy, 529 (1997).

④ 参见高秦伟:《政府规制中的第三方审核》,《法商研究》2016 年第 6 期。

⑤ 其他规制领域的类似分析,参见谭冰霖:《论第三代环境规制》,《现代法学》2018 年第 1 期。

⑥ See Xinguang Sheng, Lorrie Faith Cranor, An Evaluation of the Effect of US Financial Privacy Legislation Through the Analysis of Privacy Policies, 2 I/S: A Journal of Law and Policy for the Information Society, 943 (2006).

规制工具相互融合，使得规制既有针对性，又有实效性。[①]

以上对合作规制的内涵和样态进行了描述，其或者强调多元主体的参与，或者强调非强制行政手段及协作、平等协商方式的运用。应当讲，这些理论主张或者制度设计均具有现实意义，然而，其不足之处在于缺乏体系化、整合性的建构，从形式上看仅是多元主体、多种规范、多种方式的混杂，并未真正发挥减轻法律思维负担、法律解释以及法政策上的功能。[②] 究竟何时合作、如何合作皆成疑问，在实践操作中可能导致“合作规制”变为各方逃避责任的避风港。虽然合规规制在具体运作中强调各方主体的参与，但各方在达成合意方面存在较大困难。[③] 例如，“禁止追踪”(Do Not Track)技术就是因为企业、行业组织、用户与政府之间无法达成一致，因而效果不甚理想。[④]

有鉴于此，行政法学不能满足于对个别的法律规则和法律制度作出诠释或法政策学上的建议，还须就合作规制发生效力的条件、如何与传统法教义学相适应等问题加以深入探究。唯有以行政法学体系化方式的反思，才能让个别机制与整体制度相互衔接，才能够使行政法顺利实现既定的立法目标和秩序任务。体系化不仅要积极回应现实，还要与现实保持“必要距离”，防止便宜主义的做法；要保留必要的解释能力，否则“永远疲于应付现实变化，而未经过滤沉淀的仓促回应又时时冲击和打破它刚刚建立起的稳定和平衡”。[⑤] 展望未来，行政法学有必要从目前的过多关注多元主体的行动者中心主义转向对“规制结构”的关注。这意味着，规制研究的重心应从何者以何种方式规制何者，转变为在规制结构内，就行动者采取行为、结构如何塑造行为以及在法律框架内能否达成规制目标的讨论。在此过程中既可能利用传统的法律保留学说有效保障公众合法权益；也可以公开的要求以及合作规范的可视化使企业自我规制尽量保持竞争的中立性。由此，既可克服主体、规范、方式的混杂，又可为合作规制提供分析框架。惟其如此，在构建我国的个人信息保护制度过程中，才能够摆脱非欧即美的照搬移植思路，兼顾个人权利保护和产业发展创新，保持法律规则的开放和弹性，从而建立起符合我国社会经济发展需要的个人信息保护制度体系。

责任编辑　　谭冰霖

① See William McGeveran, Friending the Privacy Regulators, 58 Arizona Law Review, 959 (2016).

② 参见[德]施密特·阿斯曼：《秩序理念下的行政法体系建构》，林明锵等译，法律出版社 2012 年版，第 5～6 页。

③ See Mark Seidenfeld, Empowering Stakeholders: Limits on Collaboration as the Basis for Flexible Regulation, 41 William and Mary Law Review, 411 (2000).

④ See Kyle Ferden, The Swanson Paradox: Do－Not－Track and the Intersection of Data Autonomy and the Free Market, 41 The Journal of Corporation Law, 493 (2015).

⑤ 赵宏：《法治国下的目的性创设——德国行政行为理论与制度实践研究》，法律出版社 2012 年版，第 86 页。