大数据时代个人信息保护行业自律的困境与出路

Dilemma and Method on the Self-regulation of Personal Data Protection in the Era of Big Data

张继红

ZHANG Jihong

【摘　要】　随着信息产业的迅猛发展，行业自律作为个人信息保护的方式之一愈来愈受到关注。早在20世纪90年代，美国政府就鼓励以自律规范保护个人隐私。然而，实践表明自律管理机制本身存在参与度低、执行力差、缺乏有效的监督与处罚机制等问题。面对大数据、云计算等新兴技术带来的冲击，自律机制仅仅是个人信息保护的必要条件而非充分条件，政府适度介入与行业自律的有机结合才是破解当前困局的有效路径。欧盟《一般数据保护条例》即采用了行业主导、政府适度干预的理念，政府在宏观层面调控和制定个人信息保护的基本框架及原则，而市场则从微观层面发挥自我管理之基础性功能。我国目前个人信息保护领域的行业自律管理尚处于初创阶段，理应在立法先行基础上进一步扩展行业协会发挥自律作用的空间。

【关键词】　个人信息保护　行业自律　政府监管　GDPR

【中图分类号】DF49　【文献标识码】A　【文章编号】2095－9206（2018）06－0057－14

Abstract: With the rapid development of the information industry, self-regulation has become more and more concerned as one of the ways to protect personal data. As early as the 1990s, the US government encouraged self-regulation to protect personal privacy. However, practice shows that the self-regulation mechanism has problems such as low participation, poor execution, and lack of effective supervision and punishment mechanisms. Faced with the impact of emerging technologies such as big data and cloud computing, self-regulation is only a necessary condition for personal data protection, but not a sufficient condition. The combination of appropriate government intervention and industry self-discipline is the effective way to solve the current dilemma. The EU General Data Protection Regulations adopts the concept of industry-led and government-appropriate intervention. The government regulates and formulates the basic framework and principles of personal data protection at the macro level, while the market plays a fundamental role in self-regulation from the micro level. China's current self-regulation in the field of personal data protection is still in its infancy. We should further expand the space for industry associations to play a self-discipline role on the basis of legislation.

Key words: Personal data protection　Self regulation　Government regulation　GDPR

［收稿日期］　2018－09－06

［作者简介］　张继红，女，1976年6月生，上海对外经贸大学法学院教授，研究方向为金融监管法、信息保护法。

［基金项目］　国家社会科学基金一般项目“大数据时代金融消费者信息权保护制度研究”（项目编号：15BFX112）；上海对外经贸大学“一带一路”金融法制学科建设项目；上海高校智库上海对外经贸大学国际经贸治理与中国改革开放联合研究中心资助。

一、行业自律的利弊之争

作为一种有效的市场治理手段，行业自律在约束市场主体不良行为、维护市场正常运营秩序上有着自身独有的调控空间，被视为一种补充政府监管的治理路径。行业协会作为自律组织进行自我管理拥有十分悠久的历史，在很多领域的应用都极为普遍。〔1〕从理论上分析，通过自律规范整顿并构建合理的内部秩序，能够更好地实现市场有序化。相较于法律规定，自律规范更能建立“内生机制”，有效降低国家管制成本，〔2〕对于个人信息安全的维护更具专业性、针对性和可操作性。特别是当法律制度供给匮乏时，自律规范更能够灵活应对大数据、云计算等新兴技术带来的冲击和挑战，及时为行业标准提供秩序控制指导，达到早期矫正的效果。细言之，自律规范在个人信息保护方面较之法律规范具有如下优点：

（一）行业自律具有更强的制度弹性

行业自律的主要依据为自律规范。自律规范具有弹性特点，可以根据大数据时代的新特点及时进行安排，实时掌握企业及其他第三方信息收集、使用、分享的情况，进行动态跟踪。不同行业对信息的收集和处理也不一样，自律规范更具有针对性和科学性。更为重要的是，在科技创新日新月异的背景下，自律规范能够及时跟进市场创新的进度，在制定法与科技进步之间构建一张缓冲垫，通过信息保护的自觉性规范实现安全与效率的平衡。事实上，为了避免失去客户，一些网络经营者开始积极采取措施保护使用者的信息安全。〔3〕而且，自律管理有更加灵活的结构，更能适应新技术带来的变化，规则设定能够及时根据实际需要进行调整和完善。“把权力赋予自律组织进行自律性管理能够消除认证带来的官僚拖延，更有利于技术创新。”〔4〕

（二）行业自律成本更低

行业自律需要制定自律规范，并对其进行有效执行。相对于国家法律的制定及执行来说，自律规范立法及执法成本更低。传统的立法过程冗长且带有单向性，立法者并不完全知晓其所管理的行业，因此在某种程度上其所制定的管理规范并不具有实际应用价值。而且，因为技术的快速发展和进步，政府规范不能及时进行相应地调整和修改，远远滞后于现实发展，这将会进一步削弱信息的使用价值，增加企业的经营成本，大大抑

〔1〕 以金融领域为例，最早的银行业自律组织、始建于 1875 年的美国银行家协会，1891 年成立的加拿大银行公会，1919 年成立的英国银行公会，1951 年成立的德国银行联邦公会以及同期成立的法国银行同业公会，1975 年 2 月成立的巴塞尔银行监管委员会成为最具权威性的国际银行业自律组织。参见刘张君：《金融管制放松条件下银行业自律研究》，中国金融出版社 2009 年版，第 82～83 页。

〔2〕 参见鲁篱：《行业协会经济自治权研究》，法律出版社 2003 年版，第 190～193 页。

〔3〕 See Jared Strauss & Kenneth S. Rogerson, Policies for Online Privacy in the United States and the European Union, Telematics and Informatics 19, 2002, p. 173.

〔4〕 See Christodoulos Stefanadis, Self-Regulation, Innovation and the Financial Industry, Journal of Regulatory Economics 23 (1), 2003, pp. 5～25.

制数字创新。〔5〕相比之下，自律管理可以创设信息保护标准，同时避免立法的弊端，大大节约了企业合规成本。行业经营者更熟悉其经营规则，更有利于建构有效的信息保护标准。相比政府，行业协会更接近市场，能够在很大程度上克服信息传递失真问题，节约组织成员的信息收集成本，有效克服由于信息不对称导致的逆向选择和道德风险。〔6〕

自律规范作为行业经营者为了满足发展需要而共同制定的行为规则，在制定初期就历经行业内部多方利益代表充分交换意见，自律规范本身就是利益博弈与妥协的结果。对于行业经营者而言，基于共同利益，更容易接受自己行业所建立的规则。〔7〕这种较高的参与度，必然提升行业经营者对于自律规范的认可度和接受度，因此在具体执行过程中，更容易发挥其作用。从公共政策角度看，行业自律比政府监管更加迅速、有效，能够利用积累的判断力和经验解决政府较难处理的问题。〔8〕

（三）行业自律更能培育成员的诚信意识

来自于外部的政府监督，依靠刚性地、具有强惩戒性的法律手段来确保其监管规则得以执行和遵守，但这种方式明显呈现事后性、高成本、过于刚性等问题。反之，行业协会在培育成员企业的诚信意识方面具有天然优势。会员之间需要长期合作，而协会作为一种法律之外的沟通协调机制，采用集体惩戒的方式如设立行业内诚信系统，并允许其他成员企业和消费者进行查询，可以有效降低短期利益行为，增进会员企业之间的信任，形成具有正外部性的社会资本，进而促进信誉机制的形成。〔9〕正如学者指出的那样，“自律对商业活动的影响是极为深远的，而政府的控制只是一时的”。〔10〕

此外，行业自律对于本领域的市场增长、降低替代威胁和生产成本，促进行业内合作实现、增进消费者福祉等方面都有着积极意义。然而，从理论层面上分析，行业自律能否起到应有的管理效果，尚存在争议。反对者呼吁政府管理（government regulation）而非行业自律（self-regulation），认为其主要缺点可以归结为规制不足、掺杂私利、缺乏透明度等。

第一，从规则制定程序上看，行业自律规则不如法律那样严谨、规范，缺乏应有的透明度，消费者参与不够充分，因而无法提升消费者对行业自律规范的认同，公共利益也难以得到有效保护。〔11〕对于那些不参与行业自律的企业而言，甚至还存在搭便车的

---

〔5〕 See Dennis D. Hirsch, the Law and Policy of Online Privacy: Regulation, Self-regulation, or Co-regulation? Seattle U. L. Rev. 34, 2011, p. 439.

〔6〕 参见郭薇：《政府监管与行业自律：论行业协会在市场治理中的功能与实现条件》，中国社会科学出版社 2011 年版，第 161 页。

〔7〕 See Sunni Yuen, Exporting Trust with Data: Audited Self-regulation as a Solution to Cross-border Data Transfer Protection Concerns in the Offshore Outsouring Industry, Colum. Sci. & Tech. L. Rev. 9, 2007, p. 41.

〔8〕 See Robert Pitofsky, Self-Regulation and Antirust, Prepared Remarks in the D. C. Bar Association Symposium, 1998.

〔9〕 参见前注〔6〕，郭薇书，第 161 页。

〔10〕 See Margot Priest, The Privatizaton of Regulation: Five Model of Self-Regulation, Ottawa Law Review 29, 1997, p. 233.

〔11〕 See EURIM, The Role of Self-Regulation in Electronic Commerce, 1999.

现象。加之，信息行业经营者总是将个体利益凌驾于公共利益，自律管理规则不可避免地陷入宽松的怪圈。相比之下，政府管理对于信息主体权益的保护更加必要和有效。〔12〕

第二，行业自律缺乏监督和执行，更缺少有效的救济手段。自律规则的执行者并无类似于政府那样的处罚或者惩戒的权力，能否在本领域中实施自我管理的行业标准本身存在疑问。美国民主与科技中心顾问就曾指出，“行业自律明显缺乏监督和执行”，“行业制定的政策几乎没有给消费者提供有意义的救济和申诉机会”。〔13〕换言之，行业自律非但不能保护个人的信息，只会助长企业更肆无忌惮的收集、使用和转移数据。目前大多数网站经营者对于用户信息的保护，主要来自于隐私政策，即在网站上张贴隐私保护政策书面文本，赋予个人相应的选择权。然而，企业的隐私保护政策通常冗长繁杂，专业术语多不易理解，用户也没有太多耐心仔细阅读和研究。加之，个人同企业的交易过程中，往往处于弱势地位，为了获得相应的产品或服务，他们不得不将自己的信息授权给企业使用。这里的所谓“选择权”变成了不能选择的“权利”。离开了外部监管的行业自律，就相当于失去了保护的屏障，无法阻止企业利益最大化的行为。

行业自律管理的利弊之争仍在继续，孰是孰非，还需要深入个人信息保护实践进行具体分析。

二、行业自律的实践考察：以美国网络隐私保护为例

与欧盟采用综合性立法保护个人数据不同，美国采用行业自律模式保护私领域的个人隐私。在美国，除了个别领域的联邦特定立法、州立法和普通法以外，民间机构的行业规则、公司内部规章等构成个人信息保护的规范之一。〔14〕早在 20 世纪 90 年代，美国政府就鼓励并积极建议通过非政府管制的手段来保护网络隐私权。1997 年，克林顿政府公布了《全球电子商务框架》，指出“为了繁荣电子商务，私人主体应成为主导。联邦政府应当鼓励行业自律。网络应当成为竞争的自由贸易区，对于消费者的保护，不是由政府进行监管，而是由那些每天使用网络的人”。〔15〕美国联邦贸易委员会指出，随着网络和计算机技术的快速发展，“自律规范是一种侵入性最少、效率最高的方式，以保护公平的信息惯例”。〔16〕也就是说，应积极发挥市场的主导、能动作用，政府则尽可能减少干预以及实施不必要的管制措施。网络隐私工作组（The Internet Privacy Working Group，IPWG）也认为，政策和技术是网络个人隐私保护的两大支柱。而网络行业企业自律能够有效建立隐私保护政策，并向网络用户提供隐私加强型技术，如网络内容选择平台（the Platform for Internet Content Selection，PICS）的引入可以大大增强用户的隐

〔12〕 See Jody Freeman，Collaborative Governance in the Administrative State，UCLA L. Rev. 45，1997，p. 34.

〔13〕 Deidre K. Mulligan，Janlori Goldman，The Limits and the Necessity of Self-Regulation：the Case for Both，at https：//www. ntia. doc. gov/page/chapter-1-theory-markets-and-privacy，last visited on March 23，2017.

〔14〕 参见齐爱民：《大数据时代个人信息保护法国际比较研究》，法律出版社 2015 年版，第 89 页。

〔15〕 William J. Cliton & Abert Gore，Jr.，A Framework for Global Electronic Commerce，the White House，1997；Memorandum on Electronic Commerce，2 Pub. July 1，1997.

〔16〕 Federal Trade Commission，Self-regulation and Privacy Online：a Report to Congress，1999.

私保护，使其自身能够有效控制个人信息的流动。〔17〕

（一）行业自律规范

1998 年，美国联邦贸易委员会要求互联网公司建立自律规则以保护线上隐私问题。为了回应政府对行业自律的号召，许多行业的经营者都发布了指南和行业规范。〔18〕在此背景下，“在线隐私联盟”（the Online Privacy Alliance，OPA）成立，囊括了当时主要的互联网公司，如 AOL、IBM、Hewlett-Packard 等，并制定了《在线隐私权政策指南》（Guideline for Online Privacy Policies）。该指南要求所有的 OPA 成员制定“隐私政策”，提供网络用户关于其个人信息的收集及使用的基本通知，允许使用者选择退出（Opt-out）及更正错误信息，成员需采取必要措施以确保信息安全和具有可信赖性。〔19〕

但是，除了上述措施外，该指南并未禁止成员收集敏感信息，招致隐私专家 Bob Gellman 的批评。他认为指南所起的作用仅仅是“只要消费者不反对，互联网企业就可以做任何事”。〔20〕对于不遵守指南的 OPA 成员，也没有什么强制性措施。事实上，仅仅有 100 家左右的公司加入了 OPA，而一些重要的互联网企业如 Amazon.com、Lycos 则自始不参与。因为互联网公司的参与度比较低，很难说 OPA 的成立有效改善了互联网的隐私保护环境。发展到最后，OPA 也不复存在，其自身也承认自律管理的方法存在很大缺陷，开始支持线上隐私立法。〔21〕此时，美国联邦贸易委员会对于隐私保护行业自治的态度发生了大逆转，开始积极呼吁国会通过立法建立商业网站个人隐私保护的最低标准，规范企业的信息处理活动，并由专门机构监督法律施行，切实保障消费者的线上隐私问题。〔22〕

行业自律模式的另一个典型案例，就是随后建立的美国网络广告促进会（the Network Advertising Initiative，NAI）。与 OPA 参与成员涉及互联网各个领域不同，NAI 则专注于网络广告行业，并于 2000 年制定了《网络广告者的线上市场营销自律原则》（Self-Regulatory Principles for Online Preference Marketing by Network Advertisers，以下简称《自律原则》）。该《原则》对于非个人身份识别信息（Non-PII）如点击量数据以及个人身份识别信息（PII）如线下购物数据，都进行了规定。《自律原则》要求互联网广告公司在合并公开前的点击量数据与个人识别信息前，应取得用户明确的同意（opt-

〔17〕 See Deidre K. Mulligan, Janlori Goldman, The Limits and the Necessity of Self-Regulation: the Case for Both, at https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy, last visited on March 23, 2017.

〔18〕 如银行领域《银行家圆桌会议隐私原则实施计划》，建立了银行业有关个人可识别信息的隐私保护基本原则；个人咨询服务行业制定的《个人咨询服务业原则》；直营协会制定的《线上营销：隐私保护和指南》，确立了直接营销商在收集、披露和使用个人可识别信息时所应遵循的基本原则。See FEDERAL TRADE COMM'N, Privacy Online: A Report to Congress 3, 1998, at http://www.ftc.gov/reports/privacy3/toc.htm, last visited on July 8, 2018.

〔19〕 See Guidelines for Online Privacy Policies, Online Privacy Alliance, at http://www.privacyalliance.org/resources/ppguidelines.shtml, last visited on Nov. 11, 2016.

〔20〕 Ashley Craddock, Pretty Poor Privacy, Wired, June 6, 1998, at http:// www.wired.com/politics/law/news/1998/06/13256, last visited on Nov. 15, 2016.

〔21〕 参见前注〔5〕，Dennis D. Hirsch 文，第 439 页。

〔22〕 See Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace: a Report to Congress, 2000.

in）。而对于合并公开后的点击量数据与个人识别信息，则仅需要通知后选出（opt-out）即可。而且，该《原则》并未限制用户信息的二次利用，这也在实质上削弱了个人用户的隐私保护。虽然在表面上看，《自律原则》也满足了“公平信息实践惯例”的要求，即 NAI 成员需要向用户提供信息如何收集、使用及分享给第三方的通知。但是美国联邦贸易委员会的调查显示，网络用户通常无法阅读整篇隐私政策，即便阅读了，也不能完全理解其中的涵义。〔23〕也就是说，该《原则》并不能真正实现保护用户隐私的效果。

加之，《自律原则》的最大问题是如何保障成员遵守并实施。虽然该《原则》指出，将通过第三方机构的任意审计以及根据消费者投诉进行调查的方式监督该《原则》的施行情况。如果发现有成员不遵守该《原则》，将会撤销成员资格，并向社会公示。但事实上，NAI 并未贯彻这一措施。截至 2003 年，该组织的成员从先前的 12 个减少到 2 个。TRUSTe 作为第三方机构履行执行职责，一开始在其网站上还报告用户的投诉数量、问题以及处理结果等。但在 2003—2005 年期间，仅仅报告用户已经得到解决的投诉数量，而不再报告投诉数量及投诉本身。在此期间，TRUSTe 成为 NAI 的准会员，这也与一开始《原则》要求的独立的第三方机构的身份不符。〔24〕换言之，TRUSTe 无法履行独立和透明的监督职责。意识到上述问题的存在，NAI 公布了 2008 年版《原则》，虽然作了部分改进，将执行职责交还给 NAI 本身，由他自己监督成员是否遵守《自律原则》，但执行问题仍然存在。〔25〕

（二）网络隐私认证

除了行业自律规则外，网络隐私认证也是实现个人隐私保护的自律形式，其中以美国 TRUSTe 以及 BBBonline 最为典型。

成立于 1997 年 6 月的 TRUSTe，是美国第一家民间网络隐私认证机构。其主要职责在于监督会员采取的隐私保护措施，对取得会员资格的网站进行隐私政策评估和审查。任何行业的公司都可选择自愿加入 TRUSTe，并遵守客户隐私保护基本原则。TRUSTe 确保取得会员资格的企业在其网站上公布符合公平信息实践的有效隐私政策。取得 TRUSTe 的标识成为会员，必须要在其网站上说明该公司是 TRUSTe 项目的被许可人，并发布隐私声明。在隐私声明中，会员必须公布其个人信息收集情况，包括：收集了哪些信息；谁在收集信息；信息是如何使用的；信息与谁分享；向网站访问者提供有关其个人信息收集和使用的选择权；保护个人信息的安全措施及程序；网站访问者是否可以获取及更正其个人信息。同时，当用户信息的使用与收集目的不相关时，被许可企业必须向网站访问者提供禁止向第三方转移个人信息的权利。TRUSTe 则采用每季度随机抽查的方式检验其会员是否遵循已公布的隐私政策。如果有线上投诉，TRUSTe 也会启动审查程序。一旦发现会员违反其承诺的隐私政策，将会视情节轻重，或撤销该项

〔23〕报告指出，虽然很多网站的隐私政策通常会声明，其不会披露使用者的个人信息。但是，在隐私政策中存在诸多例外情形，导致个人信息实际上被经营合伙人、出资者等第三方分享和使用。参见上注。

〔24〕See Federal Trade Commission, FTC Report: Self-regulatory Principles for Online Behavioral Advertising, 2009.

〔25〕2008 年版《自律原则》对于“敏感信息”提供了更为宽泛的界定，并不利于保护个人信息。See CTR, For Democracy and Tech., Response to the 2008 NAI Principles: the Network Advertising Initiative's Self-regulatory Code of Conduct for Online Behavioral Advertising, 2008.

目的隐私认证，或提起违约合同之诉，或移送至相关的联邦执法机构。

与 TRUSTe 相近似，美国商业促进局（the Better Business Bureau，BBB）于 1999 年 3 月发起成立“BBB 线上隐私计划”（BBB Online Privacy Program）。取得 BBB 线上隐私标识的企业，必须尊重隐私并实施张贴在其网站上的隐私政策。BBB 线上隐私计划要求企业必须告知消费者信息的收集和披露情况，包括信息收集者的身份，收集信息的类型，如何使用信息以及网站采取的保护个人信息安全、准确的相关措施和程序等内容。同时，该计划的参加企业必须确保其所收集的个人信息的准确性，以及个人的信息更正权。对于基于营销目的向第三方传输个人信息，参与企业必须向用户提供选择权。BBB 线上隐私计划还专门设立了消费者信息纠纷解决机制。与 TRUSTe 类似，如果参与企业违反其隐私声明，则面临认证被撤销或被移送至相关执法机构的惩罚措施。

网络隐私认证也存在同样的困境。一是加入企业并不多，甚至有些企业不在网站上公布其隐私政策。〔26〕二是网络隐私认证的客观性受到严重质疑，特别是与出资企业存在一定的经济利益也使得网络隐私认证面临诸多指责。TRUSTe 和 BBB 线上隐私计划都属于民间非营利机构，有其出资方，而这些资助机构也是上述计划的参与企业。例如，微软就是 TRUSTe 项目的出资人，曾捐赠了 10 万美元。有人投诉微软在其 Windows98 系统中加载了认证码，能够在用户不知情的情形下收集个人信息，但 TRUSTe 则认为微软并未违反其隐私认证承诺。〔27〕

应该说，面对收集、使用和销售个人信息所带来的巨大利润，完全依赖行业自律实施个人信息保护存在较大的风险。正因为存在着严重的信息不对称，经营者自行制定的行业规范很大程度上反映了其本身的利益，容易侵害消费者的信息权利。而且，许多行业指南依赖企业自行实施，缺乏统一的强制性执行标准。〔28〕美国隐私保护自律管理的实践活动亦显示，自律组织的参与度低、会员少，执行力差，〔29〕缺乏有效的监督和处罚机制以及针对消费者的有效救济途径，企业严格遵守隐私保护自治规则的动力不足，其所在行业制定的隐私保护标准不可能充分且适当地保护消费者信息。〔30〕甚至连美国联邦贸易委员会也认为，缺乏有效的执行措施显著地削弱了行业自律规范在个人信息保护方面的施行效果。〔31〕特别是美国次贷危机之后，学界、业界的主流诉求都是要加强政府监管，人们对自律的信心丧失殆尽。世界隐私论坛更是明确指出，由各行业自发形成的

---

〔26〕 See Jonathan P. Cody, Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation? Cath. U. L. Rev. 48, 1999, p. 1183.

〔27〕 See Jeri Clausing, On-Line Privacy Group Decides Not to Pursue Microsoft Case, N. Y. TIMES, Mar. 23, 1999, at C5.

〔28〕 参见前注〔26〕，Jonathan P. Cody 文，第 1183 页。

〔29〕 See Mark E. Budnitz, Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate, S. C. L. Rev. 49, 1998, p. 847.

〔30〕 事实上，早在 1997 年欧共体的工作报告就指出，美国行业自律模式对于个人数据的保护是不充分的，因为行业自律排除了合同为基础的隐私保护以及商业行为守则。See William L. Fishman, Should the United States Meet European Demands for Greater Protection of Personal Data?, LEGAL TIMES, Sept. 15, 1997, at 29.

〔31〕 参见前注〔18〕，FEDERAL TRADE COMM'N 文。

个人数据保护自律规则最终被证明是失败的。〔32〕

多年的实证经验及教训显示，行业自律仅仅是个人信息保护的必要条件而非充分条件，面对新兴科技对现有法律制度体系的冲击，仅依赖自律机制显然捉襟见肘，只有自律机制与个人信息保护法制协同，特别是与政府监管执法密切配合，才有可能实现个人信息保护的最佳实践。

三、个人信息的有效保护：政府适度监管与行业自律的有机结合

应该说，单纯的行政监管抑或自律管理都存在固有的弊端，必须将两者的管理力量进行有机结合，才能使之在个人信息保护领域发挥最大效用。自 19 世纪末，市场万能的神话破灭，让国家干预理论大放异彩，即“有形之手”对“市场失灵”予以矫正，但国家对资源控制能力的增强必然伴随着私主体对资源支配权的弱化。已有学者在实证研究的基础上指出，完全国有化或私有化很难实现资源的优化配置，赋予主体以自我组织自我约束的能力，有时更有利于公共资源的合理分配，而这种有别于国家和市场的解决路径，或许将成为更有效率的制度安排。〔33〕信息监管体系的有序发展，有赖于自律与他律的平衡。政府监管权力过度扩张，必然挤占自律管理的空间，同时也会引发政府失灵问题。〔34〕

无论是“市场失灵”还是“政府失灵”，均表明过度管制和完全放任都会导致整个市场的紊乱。事实上，政府适度监管理念就是要避免政府过度干预市场，其责任在于顺应市场内在规律，科学制定市场运行的大体框架和原则规则，而自律管理则是政府监管之强制性立法的有益补充，能够有效发挥自我监督、自我管理的优势。随着互联网、大数据的迅猛发展，强调政府适度监管下的自律管理成为新形势下个人信息保护制度发展的一大趋势，其中以欧盟的做法最为典型。

（一）欧盟《个人数据保护指令》及成员国法

1995 年欧盟《个人数据保护指令》（以下简称《欧盟指令》）第五章专门规定“行为守则”（Codes of Conduct）。第 27（1）条规定，考虑到不同行业的特殊性，成员国和欧盟委员会应当鼓励起草有助于正确施行国内法的行为准则。换言之，行为守则的主要目的在于使得一般性数据保护立法更好地契合不同行业的特殊性。同时，如果行业协会或其他代表某一行业的数据控制人组织已经制定了国内行为守则草案，或者有意向修改或扩充现行的行为守则，成员国应当要求上述组织将草案提交给国内监管机构审查，由监管机构给出意见。监管机构应当审查行为守则草案是否与国内法律规定相一致。如果一致的话，监管机构应当征询数据主体或其代表的意见［第 27（2）条］。

---

〔32〕 See Robert Gellman & Pam Dixon, Many Failures: A Brief History of Privacy Self-Regulation, World Privacy Forum, October 14, 2011, at http://www.worldprivacyforum.org/2011/10/report-many-failures-a-brief-history-ofprivacy-self-regulation/, last visited on June 20, 2018.

〔33〕 参见毛寿龙、李梅：《有限政府的经济分析》，三联书店 2000 年版，第 171 页。

〔34〕 当国家行动不能增进经济效率或当政府把收入分配给那些不恰当的人时，政府失灵（Government Failure）就发生了。政府失灵，就是在市场经济条件下，由于自身的局限性和外部约束因素的乏力，政府在行政管理过程中所出现的负面效应。参见张建东、高建奕：“西方政府失灵理论综述”，《云南行政学院学报》2006 年第 5 期，第 83～84 页。

根据《欧盟指令》的上述规定，各成员国都在其国内法中作了相应的规定，〔35〕并要求将各行业制定的行为守则提交监管机构进行审核，以检验其内容是否与国内数据保护规则相一致。〔36〕

然而，《欧盟指令》第 27 条对于“行为守则”规定之条款较为模糊，成员国国内法对其解释及适用仍存在一定的差异性。例如，“监管机构的意见”（Authority opinion）之法律地位。有些成员国认为，“监管机构的意见”类似于“指南”，并不具有法律约束力。〔37〕另一些成员国则认为“监管机构的意见”对于监管机构本身有约束力。〔38〕而一些成员国还建立一套机制，允许行为守则具有相应的法律约束力，不仅约束监管机构本身，还对法院有约束力。〔39〕根据成员国给予各个行业制定行为守则的自由度和效力不同，又可以将其分为三种类型。〔40〕

第一类，行业主导。归入此类型的国家之国内法赋予行业在制定行为守则方面之完全的自由裁量权，突出了本行业数据控制者和数据主体的利益，相比之下监管机构的作用和影响较弱。例如，奥地利《个人数据保护法》第 6（4）条规定，法律规定的利益代表、

〔35〕 例如，荷兰《个人数据保护法》第 25（1）条规定，任何组织起草施行法律之行为准则应当特别注意该行业的特殊性。卢森堡《与个人数据处理相关的个人保护法》第 2（a）条规定，各部门应制定行为守则以确保数据保护法的正确施行。葡萄牙《个人数据保护法》第 32（1）条规定，国家数据保护委员会应当鼓励基于不同部门的特殊情形制定行为守则以促进本法的实施。

〔36〕 例如，葡萄牙《个人数据保护法》第 32（2）条规定，代表数据控制者的工会或其他团体，应当将已经制定的行为守则草案提交国家数据保护委员会征求意见。同样的，比利时《有关个人数据处理的隐私保护法》第 44 条规定，委员会应当审查提交的行为守则草案是否与本法一致。德国《联邦数据保护法》第 38a（2）条规定，监管机构应审查行为守则草案与数据保护法在数据保护方面的兼容性。卢森堡《与个人数据处理相关的个人保护法》第 32（3）（g）条规定，监管机构认为行为守则符合法律规定，应批准该守则。西班牙《个人数据保护法》第 32（3）条规定，监管当局应评估行为守则是否与法律规定一致。法国《数据处理、数据文件和个人自由法》规定，监管当局必须对行为守则的制定发表意见。爱尔兰《数据保护法》规定，委员会必须评估行为守则是否符合法律规定。

〔37〕 例如，丹麦《个人数据处理法》就规定，经批准的行为守则旨在帮助数据保护规则正确得以实施。

〔38〕 例如，西班牙《个人数据保护法》第 32（3）条规定，一旦监管机构批准了行为守则，必须在普通数据保护登记簿中进行保存和录入。如果监管机构认为行为守则不能准确表述本法，可以拒绝其进行登记，并要求申请者作必要的改变。卢森堡《与个人数据处理相关的个人保护法》第 32（3）（g）条规定，监管机构应当批准提交的行为守则；爱尔兰《数据保护法》第 302 条规定，监管当局的肯定性意见应当视为《一般行政性条例法案》之决定的涵义；葡萄牙《个人数据保护法》第 32（3）条规定，监管当局应宣布行为守则草案是否与法律规定相一致，监管机构以决议形式所做的宣告行为构成“有约束力的行政性决定”。

〔39〕 例如，意大利《个人数据保护法典》第 186 条规定，监管当局必须在意大利官方杂志上公布已经得到批准的行为守则。已公布的行为守则构成针对某一行业数据控制者具有法律约束力的行为规范。同样的，爱尔兰《数据保护法》也规定，司法部可以将已经获得批准的行为守则提交给议会以获得进一步许可。如果议会同意了该行为守则，相应地，守则取得法律效力，类似于强制性法律规定，其规则条款也被视为与法律条款具有同等约束力。英国 1998 年《个人数据保护法》第 52（3）条规定，专员应向议会两院分别提交行为守则。

〔40〕 参见前注〔5〕，Dennis D. Hirsch 文，第 439 页。

专业协会或其他类似机构可制定该行业的行为守则。〔41〕需要注意的是，此类型中虽然国内数据保护法允许行业自行制定行为守则，但并不积极推动其必须制定相应守则。如果该行业不制定行为守则，则应遵守其国内数据保护法的一般性规定。如果制定行为守则，监管机构必须审查其是否与国内法相一致，并给出审查意见。同时，法院有权对监管机构的意见进行司法审查。换言之，行业协会、公司或公民团体都可以对监管机构有关行为守则是否符合法律规定寻求司法救济。

第二类，共同协商。归入此类型的国家，其国内法要求监管当局鼓励各行业制定行为准则，制定过程应与监管者进行协商。也就是说，监管机构与行业之间需要密切合作，以共同推动行为守则的出台。例如，希腊《与个人数据处理相关的个人保护法》第 19（1）条规定，监管机构应鼓励并帮助协会或其他组织制定行为守则。〔42〕通常情形下，此类型的成员国法允许行为守则上升为有约束力的法律规则。而且，监管机构会强烈建议行业制定数据保护标准更高的行为守则。〔43〕

第三类，政府主导。此类型的成员国监管机构会推动行业制定行为守则，如果协会不制定的话，则由监管机构来制定并施行于某一行业。例如，爱尔兰《数据保护法》第 8 条规定，如果专员认为行为守则是有益的但行业没有制定，则专员在咨询相关协会和相关利益方之后可以自行制定行为守则。〔44〕显然，此种类型的成员国立法，监管机构在推动和制定行业守则的力度上是最大的。罗马尼亚《与个人数据处理和数据自由移动有关的个人保护法》更为严厉，要求行业协会“有义务制定行为守则并提交监管机构以便其审查”［第 28（1）条］。监管机构应决定是否批准该守则，而不是仅仅发表相应的意见。事实上，上述规定增加了监管机构的审核、评估义务，获得批准的行为守则的约束力也较强。〔45〕

（二）《一般数据保护条例》（GDPR）的最新发展

2018 年 5 月 25 日正式生效的 GDPR 在很大程度上克服了《欧盟指令》存在的缺陷，在欧盟成员国创设了相同水准的数据保护标准，被称为史上最严格、保护水平最高的数据保护规则。与《欧盟指令》需要转化适用不同，GDPR 一旦生效，其约束力将突破成员国层面，立即构成成员国国内法律体系的一部分。在其第四章第 5 部分专门规定了“行为守则和认证”（Codes of Conduct and Certification）。第 40 条规定，各成员国、监管机构、数据

〔41〕同样的，比利时《有关个人数据处理的隐私保护法》第 44 条、丹麦《个人数据处理法》第 74 条、芬兰《个人数据法》第 42 条、德国《联邦数据保护法》第 38a 条、荷兰《个人数据保护法》第 25（1）条，都授权行业组织制定行为守则。

〔42〕与之相类似，意大利《个人数据保护法典》第 12 条规定，格然特应鼓励制定不同领域的行为守则和专业实践，并验证其是否符合法律和条例规定；葡萄牙《个人数据保护法》第 32 条规定，监管当局应鼓励制定行为守则；马耳他《数据保护法》第 40（g）条规定，专员应鼓励各部门制定行为守则。

〔43〕例如，1999 年葡萄牙数据保护机构通过了一个正式的决议，要求部门制定的行为守则应有助于在各具体行业更严格地执行数据保护法的相关规定。也就是说，行为守则的数据保护标准相比数据保护法更高。

〔44〕同样的，英国 1998 年《个人数据保护法》第 51（3）条授权专员在与商会、数据主体或其认为适当的能够代表数据主体之组织进行协商后，准备并披露相关良好做法之行为守则。

〔45〕参见前注〔5〕，Dennis D. Hirsch 文，第 439 页。

保护理事会以及欧盟委员会应鼓励制定行为守则，以推动本条例更好的适用。行为守则的制定应考虑不同行业数据处理者的特殊性，特别是微型、小型以及中型企业的需要。为了使本条例得以具体应用，各协会及代表不同类型的数据控制者或处理者可以起草、修订或扩充现有的行为守则，具体包括：公平透明的处理；具体行业数据控制者所追求的合法利益；个人数据的收集；个人数据的虚假信息；提供给公众及数据主体的信息；数据主体权利行使；有关儿童的保护以及父母同意下的信息收集；数据安全措施；数据泄露后向监管机构和数据主体进行通知；个人数据传输到第三国或国际组织；数据主体与控制者冲突解决的庭外程序等。

正是《欧盟指令》规定条款的模糊，导致各成员国在具体适用过程中对指令内容的解释不一。基于此，GDPR 对监管机构与行业协会在制定守则的权力分配上作了明确规定，由行业协会或其他机构制定、修改或扩充行为守则，提交至监管机构。监管机构针对该守则是否符合本条例发表意见；如果认为守则提供了充分、适当的保护，监管机构应批准守则草案［第 40（5）条］。获批的行为守则，由监管机构进行登记和公告［第 40（6）条］。

如果行为守则涉及其他成员国的数据处理活动，则监管机构在批准该守则之前，应提交至数据保护理事会。理事会就行为守则是否符合本条例发表意见，如果认定其提供了适当的保护，理事会应向欧盟委员会提交该意见，由欧盟委员会决定是否批准该守则。一旦批准，行为守则在欧盟境内都有普遍约束力。理事会应对已经获得批准的行为守则进行整理和登记，并采取适当的方式进行信息公开［第 40（7）（8）（9）（11）条］。

关于行为守则施行情况的监督，则可由监管机构委托授权该领域具有相当水平的专业机构开展监督活动。该监督机构，应当证明其在某个领域具有独立性和专业性；建立适用守则之合格数据控制者和处理者的评估机制和程序；建立针对违反守则的控制者和处理者之投诉程序，并使该程序向数据主体和公众进行公开；向监管机构证明其履行监督职责不会产生利益冲突以及数据控制者或处理者违反守则可以采取的适当措施。监管机构发现监督主体不再满足上述条件，则可以撤销其监督授权（第 41 条）。

应该说，在行为守则的制定上，GDPR 更倾向于行业主导、监管机构适度干预的理念。对于行为守则实际执行情况，各成员国监管机构也不直接作为监督者和管理者，而是可以委托授权独立的第三方机构施行监督权，更加强调和突出市场自我管理的重要性，监管机构则可以将精力集中于自身的数据保护职责，充分平衡了政府和市场的监督力量。换言之，欧盟为代表的个人信息保护路径，不仅强调成员国数据保护机构积极鼓励行业协会制定行为守则，还主动促进形成适用于欧盟市场的某一行业统一的自治规范，政府在宏观层面调控和设计个人信息保护基本原则及规则，而市场则从微观层面积极发挥自我管理之基础性功能，充分调动其主观能动性。在大数据、移动互联网等技术手段的不断推进下，政府与市场则遵循技术中立原则，鼓励研发和推广信息保护型的处理技术。

GDPR 另一个突出贡献，就是正式引入原来完全处于自发状态的数据标识和认证制度。第 42 条规定，考虑到微型、小型及中型企业的特殊需要，应鼓励建立数据保护认证机制与数据印章、标识制度，以证明数据控制者和处理者的数据处理活动遵守本条例的规定。这种认证应当是自愿的，且程序是透明的。颁发给数据控制者或处理者的认证

时效，最长不超过 3 年，可以申请续展。如果认证机构认为其不再符合相关条件时，该认证将被撤回。数据保护理事会整理所有的认证机制和数据保护印章及标识，并予以登记和公告。第 43 条规定了认证机构的具体要求。认证机构应当具有在数据保护方面的专业知识和经验。认证机构应由监管机构或符合欧盟第 765/2008 号规定的国内授权主体委托授权，从事颁发认证标志以及认证续展的相关活动。与行为守则的监督机构相类似，认证机构也需要符合一定条件（诸如证明其在认证方面具有独立性和专业性，认证标准得到监管机构或理事会的批准，建立了颁发认证标识、定期审核和撤销认证标识等的程序，建立了数据控制者或处理者因违反认证的投诉程序以及证明其履行认证职责不会导致利益冲突等），才能获得认证授权。这种认证授权的最长期限是 5 年，届满并符合条件可以申请续展。欧盟委员会可以制定有关认证或数据保护标识之技术标准。

虽然认证制度在一定程度上存在着运营成本，需要建立独立的、不产生利益冲突的认证机构，监管机构还要对其进行委托授权；为了取得认证标识，企业需向认证机构缴纳一定的认证费用；认证机构也需要深入企业内部进行数据保护方面的评估，以评判其是否符合颁发认证标识的条件等，均有相应的人力、物力以及技术投入。但是，这种认证和标识制度充分调动了市场监督力量，大大节约了监管机构的外部监督成本，对于消费者而言更容易辨识提供相同或近似产品或服务的企业在数据保护方面存在的差异。取得数据保护认证标识的企业，意味着其在数据保护领域符合现行法律规定，个人数据保护水平较高，从而大大增加了客户的认同度。特别是对于那些小微企业，取得认证在很大程度上代表着在市场中能够更容易获取客户的信任和支持。相反，那些没有取得认证或者认证失效或被撤销的企业，消费者可以选择用脚投票，由此形成源自市场的有效监督，督促作为数据控制者或处理者的企业提升自身的数据保护水平。

四、我国个人信息保护的自律管理现状及模式选择

我国目前尚无个人信息保护的专门法律，主要采用部门立法的方式分领域来保护个人信息；行业自律管理也仅处于初创阶段，涉及个人信息保护的自律规则并不多见。

互联网领域，中国互联网协会发布《中国互联网行业自律公约》（2004）、《博客服务自律公约》（2007）等，对互联网信息服务自律作了规定，但其主要规范网络信息内容是否合法、健康，有无侵害知识产权等，并未涉及个人信息保护。仅在《互联网搜索引擎服务自律公约》（2012）第 10 条规定，搜索引擎服务提供者有义务协助保护用户隐私和个人信息安全，收到权利人符合法律规定的通知后，应及时删除、断开侵权内容链接。

金融领域，笔者检索了中国证券业协会、中国保险业协会以及中国银行业协会公布的自律公约及其他自律规则，并未发现投资者、投保人和被保险人以及银行客户信息保护方面的具体规范和措施。中国银行业协会在 2012 年 3 月 16 日发布了一个“敦促会员银行进一步加强客户信息安全管理”的公告，起因也是源于中央电视台“315”晚会报道个别银行泄露客户信息，因而银行业协会督促相关会员银行进行核实，并要求会员银行进一步加强对客户信息的管理和保护，以强化内控合规管理。

作为全国性互联网金融行业自律组织——中国互联网金融协会，于 2016 年 3 月公

布《中国互联网金融协会会员自律公约》（以下简称《自律公约》），共四章 22 条，第 7 条专门就会员应履行的金融消费者权益保护义务作了规范，其中明确了互联网金融企业会员“应当保证客户信息安全，防止信息的灭失、毁损与泄露，不得利用客户信息从事与客户约定事项外的活动”。

从上述行业协会的自律规范内容看，应该说，我国通过行业自律规范实施个人信息保护的总体水平较低，目前仍处于起步阶段，尚未作为行业自律规范的一项主要内容。仅有的规定，也异常简单、笼统，并未有具体实施细则和保护措施，与欧美等国相比明显滞后。

总体而言，虽然我国逐步扩大了各领域行业自律组织进行自我管理和约束的权限，但并未根本性改变其受来自政府、行政监管当局管控的本质，独立性被严重弱化。行业协会的行政色彩浓厚，不仅行业协会是由政府及监管者推动形成，而且其代表政府意愿的程度远远高于代表其行业内部成员，自律管理“公权化”现象十分突出。〔46〕换言之，我国行业协会承载的多种角色——政府的辅助者、成员利益的代表者、行业自律管理者，特别是充当政府监管机构在各个行业施行行政权力的某种“代理机构”，使其与其他角色产生一定的冲突。正是角色冲突，导致自律管理的独立性严重缺失，无法实现对成员利益和行业利益的维护，在一定程度上降低了行业协会在本领域内的公信力。

自律组织就其法律属性而言，可归为社会团体法人，属于私主体范畴的民间机构。目前，我们更需要进一步完善和强化的就是使其回归本位、角色矫正。也就是说，应当确保行业协会之独立性且不被异化，政府应作适当干预，而非取而代之，有效发挥其自我管理的积极作用。如何在个人信息保护领域划分自律管理与政府监管之权力边界，不仅将影响个人信息保护的实效，同时也直接决定着自律组织的生存环境和发展空间。

倘若政府监管力度过强、范围过广，必然挤压并抑制行业自律管理的发展，无法充分体现其独立的话语权。而我国一直贯彻“政府主导型”的监管理念，包括各行业经济改革的主要推动力量仍然来自强大的政府，“大到游戏规则的制定，小到市场准入的审批、公司市场行为与行政运作、机构负责人的任免甚至日常教化、知识培训等都不遗余力地被承揽下来”。〔47〕而且，我国的经济发展道路也与西方国家存在明显差异，特别在自律管理方面缺乏经验，更重要的是市民社会自治精神缺失。行业协会作为市民社会的基础性力量，有助于克服市场失灵，也是社会制约权力的重要力量。〔48〕

政府的权力扩张，虽然在一定程度上确实能够快速培育相关市场并建立秩序基础，但也使得市场参与主体不能完全独立运营，特别是无法培养成熟、理性的从业者。政府

---

〔46〕 以中国互联网金融协会为例。2015 年 7 月 18 日，中国人民银行等十部委联合印发了《关于促进互联网金融健康发展的指导意见》（银发［2015］221 号），明确提出“人民银行会同有关部门，组建中国互联网金融协会”。随后，人民银行牵头，各金融监管部门参与，中国互联网金融协会正式挂牌成立。中国互联网金融协会在其章程和自律公约中都反复强调在“中国人民银行的指导下”，将发挥行业自律机制在规范互联网金融企业的市场行为、维护市场秩序、防范系统性风险以及保护金融消费者等方面的积极作用。

〔47〕 廖志敏：“纠缠于行政与司法——中国股市监管的现状与未来”，载《金融法苑》（2003 年第 1 期），法律出版社 2003 年版，第 68 页。

〔48〕 参见鲁篱：“行业协会社会责任与行业自治的冲突与衡平”，《政法论坛》2008 年第 2 期，第 95 页。

不仅需要承担本应由市场主体自行承担的经营风险和责任，还可能遏制市场的创新活力。事实上，行业自律是个人信息保护不可或缺的重要组成部分，虽然其作用的发挥有赖于多种外部条件和环境的制约。行业协会在建立之后，政府可以对其自律活动进行指导，但不能干预过度。要想使自律机制真正发挥作用，必须处理好政府与协会之间的关系。

应该说，任何一种市场治理主体都有其优势和局限性，单独依赖任何一方都是不够的。而现阶段政府如何放权于市场，将自律管理权力还给自律组织，将是改变行业协会自律管理“公权化”问题的关键。在此基础上，各领域的行业协会可以根据不同企业的实际经营情况，制定相应的“消费者或客户信息保护指引”以具体指导会员机构强化并完善个人信息保护的内控制度，将信息安全理念进一步融入其日常经营活动，切实发挥自律管理实效。同时，鉴于行业协会所代表的会员利益可能与公共利益之间存在着一定偏差，对行业实施监督又是政府监管机构所必须履行的职责，应由政府监管机构从外部对行业进行奖惩激励，确保其监管措施的威慑力，以强制性矫正行业协会不自律或自律不足的行为。

结语

在技术创新不断的信息领域，政府监管具有一定的刚性和信息滞后性，但行业自律亦存在问题。虽然在市场信息的获取方面，行业协会较监管机构更为及时和充分，但自律规范不可避免地带有“私利性”，甚至有些规范偏离了个人信息保护的初衷，需要政府监管予以矫正。来自欧美的经验及教训表明，上述两种管理手段需相互促进、互为补充，特别是在个人信息保护的目标驱动下，才能发挥更大作用。

反观我国，自治精神严重缺位，个人信息保护法律基础十分薄弱，绝大多数领域的行业协会都在政府扶持下建立，而非“自下而上”在行业自身客观需求的基础上自发产生。不仅有关信息保护的自治规范少之又少且难以细化，亦缺乏行业内部推动实施的内在动力，更无有效的信息纠纷解决机制。而且，企业和个人的信息保护意识欠缺。有鉴于此，现阶段试图以行业自律为主导实施个人信息保护明显力有不逮。目前还需从立法层面强化对个人信息的保护，制定专项法律并设立统一的信息监管机构，而非现在的多头监管、九龙治水。同时，以成文法为基础，鼓励各行业协会积极参与个人信息保护行为规范的制定和执行，辅之以政府指导，从而逐步提升个人信息保护的实效性。

参考文献

［1］鲁篱．行业协会经济自治权研究［M］．北京：法律出版社，2003.

［2］刘张君．金融管制放松条件下银行自律研究［M］．北京：中国金融出版社，2009.

（责任编辑：刘　权　赵建蕊）