编者按：《法学研究》2017年秋季论坛于10月21日在上海召开。本次秋季论坛以“个人信息使用与保护的法律机制”为题，与会学者围绕个人信息权的概念、内涵界定与类型，个人信息的法律保护模式及其转变，大数据时代个人信息的权属及其限制，个人信息的可交易性及其治理机制，大数据在刑事司法中的应用等诸多议题，从法理学、行政法、民法、商法、知识产权、刑法、刑事诉讼法等多个学科视角展开了密集讨论。论坛得到了中国社会科学院国际法研究所、中国人民大学、厦门大学、华东政法大学、中央财经大学、北京航空航天大学等科研机构、高校专家学者的热情响应和积极参与。为及时反映论坛研讨成果，《法学研究》本期从众多征文中遴选四篇论文先行刊发，以飨读者。论坛的其他重要成果也将陆续刊出。

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

周汉华 *

内容提要：在大数据时代，信息控制者对于个人信息有很强的利用激励而缺乏同等程度的保护激励。如果法律规则只是简单施加各种禁止性或者强制性规定，势必因为激励不相容影响有效实施。尽管立法模式不同，不论欧盟还是美国，近年来都在探索建立激励相容的个人数据治理体系。我国目前的个人信息保护相关立法存在法律要求与信息控制者内部治理机制脱节、刑法制裁与其他法律手段脱节、责任规范与行为规范脱节等问题。个人信息保护法应以培育信息控制者内部治理机制为目标，以构筑有效的外部执法威慑为保障，促使信息控制者积极履行法律责任，并对违法行为予以制裁。个人信息保护法应确认信息主体在公法上的个人信息控制权，不能也不应该回避基本权利话语。个人信息保护法的实施，需要先从信息安全风险管理角度切入，由易到难，循序渐进，推动激励相容机制实现。

关键词：激励相容　个人信息保护法　个人信息控制权　信息安全风险　大数据时代

一、以激励相容为制度设计的核心

国内外学术界对于中国改革开放基本经验的主流总结，无外乎中央与地方关系上的纵

* 中国社会科学院法学研究所研究员。

作者分别在2017年召开的阿里巴巴“云栖大会数据安全生态专场”和中国政法大学中欧法学院“大数据时代的个人信息保护国际学术讨论会”上发言，阐述本文主要观点并得到积极回应、建议，作者对相关专家再次表示衷心感谢。

向分权改革和政府与市场关系上放松管制的市场化改革。“我国经济体制改革最核心的内容就是实现由传统的计划经济向社会主义市场经济体制的转轨”,〔1〕国家通过分权与市场化改革,调动地方政府与市场主体的积极性与创造性,形成推动经济发展的巨大合力。不同的理论解释,内在逻辑均是强调通过激励机制调整来调动各级政府或者市场主体的积极性与创造性,走出一条中国的大国发展道路。〔2〕与经济发展相适应,中国社会治理变迁的主要方向,也是“从一元治理到多元治理、从集权到分权、从人治到法治、从管制政府到服务政府、从党内民主到社会民主”。〔3〕从管理到治理的转变,蕴含的是多元主体的互动、协商与合作,而不再仅仅依靠过去自上而下单方面的控制与命令。〔4〕

中国发展道路选择不仅符合本国国情,也与近年来国际上政府改革的普遍经验契合。〔5〕20 世纪 70 年代末以来,全球范围掀起了汹涌澎湃的行政改革浪潮,被称为新公共管理运动,其基本特征包括公民为本、市场化、结果导向、分权协作、民主参与、多中心自主治理等。〔6〕新公共管理运动的实质是基于激励约束机制,构建多方合作治理的有效格局。学术界认识到,“与高度复杂性和高度不确定性的时代相适应的社会治理模式应当是一种合作行动模式,只有多元社会治理主体在合作的意愿下共同开展社会治理活动,才能解决已出现的各种各样的社会问题,才能在社会治理方面取得优异的业绩”。〔7〕

传统法律理论认为,法律是主权者的命令,是必须遵守的规范,令行禁止是其基本特征。因此,传统立法规制方式通常是命令控制方式,表现为禁止性规范或者义务性规范,要求被管理对象不得或者必须为某些特定行为。这种规制方式有很多弊端,包括:要求很强的执法能力,否则命令会被普遍漠视;由于信息不对称,这种命令可能与市场规律脱节,遏制市场主体创新能力与守法诱因;执法部门权力过大,可能会导致选择性执法或者“执法捕获”等问题。在全球行政改革浪潮中,传统的命令控制式规制受到广泛批评,激励性监管得到重视,人们发现规则如果能够与被管理者激励相容,会极大降低执法成本,提高合规动力。〔8〕因此,法律规则除了命令、禁止以外,还可以发挥引导作用,调动被管理者

〔1〕 国家发展改革委经济体制综合改革司、国家发展改革委经济体制与管理研究所:《改革开放三十年:从历史走向未来》,人民出版社 2008 年版,第 91 页。

〔2〕 对于经济分权与经济发展的激励结构的分析,参见王永钦等:《中国的大国发展道路——论分权式改革的得失》,《经济研究》2007 年第 1 期,第 5 页;对于财政分权理论的发展脉络与经验研究,参见张军:《分权与增长:中国的故事》,《经济学(季刊)》2008 年第 1 期,第 21 页;对于市场化改革改善企业的激励机制带来微观生产效率提高的实证解释,参见樊纲、王小鲁、马光荣:《中国市场化进程对经济增长的贡献》,《经济研究》2011 年第 9 期,第 4 页。

〔3〕 俞可平:《中国治理变迁 30 年(1978—2008)》,《吉林大学社会科学学报》2008 年第 3 期,第 5 页。

〔4〕 “由过去那种以行政命令为核心的自上而下单向式的施政方式,逐渐向政府与公民对话沟通双向互动式的施政方式转变。”周光辉:《从管制转向服务:中国政府的管理革命——中国行政管理改革 30 年》,《吉林大学社会科学学报》2008 年第 3 期,第 24 页。

〔5〕 对于西方国家新公共管理运动的评述,参见陈振明:《评西方的“新公共管理”范式》,《中国社会科学》2000 年第 6 期,第 73 页。

〔6〕 参见周志忍:《当代政府管理的新理念》,《北京大学学报(哲学社会科学版)》2005 年第 3 期,第 103 页。

〔7〕 张康之:《论主体多元化条件下的社会治理》,《中国人民大学学报》2014 年第 2 期,第 6 页。

〔8〕 参见[美]朱迪·弗里曼:《合作治理与新行政法》,毕洪海等译,商务印书馆 2010 年版,第 25 页;[美]史蒂芬·布雷耶:《规制及其改革》,李洪雷等译,北京大学出版社 2008 年版,第八章。对于命令控制式规范、基于绩效的标准和基于激励的制度三种规制方式的分析,以及从命令控制式向基于激励监管的趋势改变,参见 Jon D. Hanson & Kyle D. Logue, *The Costs of Cigarettes: The Economic Case for Ex Post Incentive-Based Regulation*, 107 Yale L. J. 1173 (1998)。

的守法诱因。如何设计这种激励相容机制，是规范实施的成败关键。〔9〕

理论研究与国内外实践发展均表明，政策或者立法如果激励不相容，会形成“管理型”立法，而不是“治理型”立法。〔10〕这样制定出来的政策或者法律，实践中难以得到执行，〔11〕还可能导致执行成本高、规制对象抵触、执行效果差、执行权威受损、运动式执法、选择性执法甚至执行部门造假等连锁问题。〔12〕在我们“所制定的法律、法规中，绝大多数事实上没有被当作法看待，没有起到法所应起的作用”，首要根源在于“立法违背科学，或立法技术存在问题，使法不能实行或难以实行”。〔13〕

我国制定个人信息保护法，不能脱离大的制度背景，有必要从中国改革开放的基本经验和全球行政改革的大趋势中吸取养分，避免或者少走弯路。在大数据时代，由于数据本身的特性，信息控制者有很强的利用激励而缺乏同等程度的保护激励。如果法律规则不能因势利导，只是简单施加各种禁止性或者强制性规定，势必因为激励不相容影响有效实施。

随着信息技术发展，数据传输、储存、计算成本快速下降，数据开始成为资源。大数据不仅具有容量大、类型多、存取速度快等特点，还可以通过分析技术“使数字信息成为知识，支持智能决策”，〔14〕产生新价值。这样，大数据不仅给信息控制者带来巨大经济收益，也给消费者（包括信息主体）带来免费使用、高品质服务、快速迭代创新等各种便利。〔15〕凯文·凯利在对未来20年商业科技发展预测的一次讲演中提出，在大数据时代，“所有生意都是数据生意”，“个人数据才是大未来”。〔16〕舍恩伯格更明确指出，“大数据的核心就是预测”。〔17〕在大数据时代，数据对于信息控制者而言，就是生产要素和行动指引。信息控制者必然会充分利用大数据揭示的相关性，提前预测信息主体和社会的各种需要，提供精准的定制化产品或服务。对于国家而言，数据早已成为各国基础性战略资源，大数据发展成为国家战略的一部分。〔18〕

---

〔9〕 对于不同领域激励相容机制设计的讨论国内外都不少见。See Inara Scott, *Incentive Regulation, New Business Models, and the Transformation of the Electric Power Industry*, 5 Mich. J. Envtl. & Admin. L. 319 (2016)；陈思、罗云波、江树人：《激励相容：我国食品安全监管的现实选择》，《中国农业大学学报（社会科学版）》2010年第3期，第168页；蒋海、萧松华、齐洁：《金融监管效率的基石：激励相容的监管机制》，《当代经济科学》2004年第4期，第15页；Ian Ayres & Matthew Funk, *Marketing Privacy*, 20 Yale J. on Reg. 77 (2003).

〔10〕 有学者指出，“过去的许多立法更多地体现了管理甚至管制的思想，对政府权力强调过多，而对市场主体的权利关注不够”。张守文：《政府与市场关系的法律调整》，《中国法学》2014年第5期，第69页。

〔11〕 对于政策制定科学性与执行有效性关系的讨论，参见丁煌：《政策制定的科学性与政策执行的有效性》，《南京社会科学》2002年第1期，第38页。

〔12〕 周雪光从组织学角度分析了我国政策执行偏离初衷、基层政府部门共谋造假现象的制度根源，提出“组织中激励设计的目的是诱导有利于组织目标的行为。但是，如果激励设计不当，就会导致与组织目标相悖的行为”，“在激励与组织目标不一致的情况下，正式激励机制力度越大，目标替代的现象越严重，共谋行为的驱动力便越强”。用该理论分析一些看似严厉的法律规定在实践中普遍面临的执行困境，也非常有说服力。周雪光：《基层政府间的“共谋现象”——一个政府行为的制度逻辑》，《社会学研究》2008年第6期，第13页，第15页。

〔13〕 周旺生：《论法之难行之源》，《法制与社会发展》2003年第3期，第17页。

〔14〕 Martin Hilbert, *Big Data for Development: A Review of Promises and Challenges*, 34 Dev. Policy Rev. 139 (2016).

〔15〕 See D. Daniel Sokol & Roisin E. Comerford, *Antitrust and Regulating Big Data*, 23 Geo. Mason L. Rev. 119 (2016).

〔16〕 http://www.360doc.com/content/14/1028/19/471722_420674983.shtml，2018年1月6日访问。

〔17〕 ［英］维克托·迈尔—舍恩伯格、肯尼思·库克耶：《大数据时代：生活、工作与思维的大变革》，盛杨燕、周涛译，浙江人民出版社2013年版，第16页。

〔18〕 国务院发布的《促进大数据发展行动纲要》明确提出，大数据成为推动经济转型发展的新动力，重塑国家竞争优势的新机遇，提升政府治理能力的新途径。

大数据由人、机器或者传感器产生。其中，最基本、最有价值的是个人信息，由用户活动产生，“收集和整理个人信息都是获取权力的方式，通常以信息主体为代价”，〔19〕因此需要在个人信息保护与大数据发展之间实现平衡。不同于其他生产要素，数据具有公共产品才具有的非排他性、非独占性特点，可以反复使用、共享，〔20〕这使信息控制者对个人数据保护远不如对其他私有财产保护重视，容易产生各种疏忽现象。在网络环境下，数据具有随时产生、多点存储、多次开发、跨场景应用、多人经手、跨国界传输、收集与处理分离、生命周期短、孤立数据本身并不产生价值、需要技术解决方案等特点，〔21〕若全部都加以保护，技术、经济上有很大难度，会产生很高的保护成本。并且，隐私与隐私之间也需要权衡，在一端加强对隐私的保护，会在另一端产生弱化对其保护的结果。〔22〕数据发生泄露的情形非常复杂，〔23〕个人数据滥用的受害者是信息主体，不是信息控制者。信息控制者很难有充分的激励与能力保护个人数据，只是被动应付法律要求。

在信息控制者利用激励与保护激励明显失衡的结构下，如果缺乏外部干预与政府监管，势必产生“丛林法则”和对个人信息的肆意滥用，〔24〕这是各国普遍重视个人信息保护、个人信息保护法成为全球性立法趋势的根本理由。我国近年来也明显加强了立法与制度建设的步伐，从多方面加强对个人信息的保护力度。但是，在信息控制者激励失衡的背景下，如果立法缺乏科学性，只是简单施加各种强制性外部要求，忽视信息控制者内在激励机制设计，并不能消除失衡根源。从概率角度看，利用与保护之间失衡的可能性仍然很大，占四分之三的比例：外部监管过于严格，抑制大数据开发利用；缺乏监管或者监管要求普遍不被遵守，大数据利用以牺牲个人信息保护为代价；监管游移不定，忽左忽右，陷入既没有大数据利用也难以保护个人信息的双输格局。只有外部要求与内生激励相容，才能够实现大数据利用与个人信息保护协调发展，其概率只有四分之一。

在大数据时代来临之前，个人数据实际处于未被利用的沉睡状态，激励失衡问题并未被激活。至大数据时代，随着数据价值逐步被认识，信息控制者利用数据的激励越来越强烈，激励失衡现象会愈发突出，法律实施遇到的挑战也会越来越大。因此，大数据时代的个人信息保护，绝不仅仅是制定个人信息保护法那么简单。真正的挑战在于，如何通过科学的立法与制度设计，理顺立法要求与信息控制者内在激励之间的关系，使个人信息保护成为信息控制者的内在需要。这是个人信息保护法制度设计的目标和最终评价标准。

---

〔19〕 A. Michael Froomkin, *The Death of Privacy*, 52 Stan. L. Rev. 1462 (2000).

〔20〕 “使用数字信息，不存在耗尽问题”，可以几乎无成本快速复制。这些特征使数字信息成为（几乎）免费、精确、实时的资源。See Eric Brynjolfsson & Andrew McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, W. W. Norton & Company, 2014, p. 62.

〔21〕 对于数据特点的全面分析，参见前引〔14〕，Martin Hilbert 文，第 135 页以下。

〔22〕 See David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. Chi. L. Rev. 246 (2016).

〔23〕 美国 Verizon 公司的研究报告将数据泄露的情形分为九种，分别是犯罪软件、网络间谍、拒绝服务、内部人以及特权滥用、其他错误、支付卡读卡器、销售点入侵、物理盗窃与损失、网络应用供给。See Verizon, *2017 Data Breach Investigations Report*, 38 (2017).

〔24〕 具体事例参见［美］弗兰克·帕斯奎尔：《黑箱社会：控制金钱和信息的数据法则》，赵亚男译，中信出版集团 2015 年版，第二章。

二、准确理解欧美个人信息保护法的新发展

欧盟与美国个人信息保护法律路径不同，两种模式的差异是客观的，也是明显的。〔25〕但是，国内过去比较欧美个人信息保护法律，普遍缺乏对两种模式实际运行状况以及共性的研究，存在简单的扬美抑欧现象。不少人认为欧盟国家不重视大数据发展、美国不保护个人隐私，〔26〕并将制定个人信息保护法与阻碍创新（欧盟模式）画上等号，〔27〕将不保护隐私与更有利于创新（美国模式）画上等号，〔28〕人为制造了隐私保护与创新不可兼得的两难局面。这种贴标签式的研究方法，既限制了比较研究的深度和广度，与现实情况存在很大出入，更改变不了美国经验无法学、欧盟引发的国际立法趋势无法逆转的大格局。其实，大数据发展与个人信息保护的平衡作为这个时代的最大挑战之一，〔29〕欧盟与美国分别面临各自的问题，都难言找到了完美的解决方案，〔30〕对后发国家最重要的是要从欧美的经验与教训中探索个人数据治理的成功之道。

随着大数据时代来临，从实证出发，探讨个人信息保护的有效实施机制，而不仅仅是关注法律规定的差别，已经成为近几年国际上、尤其是美国隐私法律研究的新热点。不论名称叫新治理、合作规制、合作治理还是叫回应性规制、激励规制等，其背后的机理均在于发现有效的激励机制，调动被管理对象参与治理的积极性，提高执法效果。最新国际实证比较研究成果表明，欧美两种模式实际上存在某些共同规律可循，而欧盟不同国家之间的差别也比过去想象的要大得多；不管哪种模式，不论法律多么严格，只有激励相容才会取得预期保护成效，不相容则难以得到执行，〔31〕甚至会导致既阻碍创新又保护不了个人信息的双输结果。〔32〕因此，成败的关键不在于法律规定的模式差别，而在于个人数据治理的

〔25〕 对于欧盟与美国在隐私保护法律上的异同及其演变过程的介绍，参见 Paul M. Schwartz, *The EU-U. S. Privacy Collision: A Turn to Institutions and Procedures*, 126 Harv. L. Rev. 1966 (2013); Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 Stan. L. Rev. 1318 (2000)。

〔26〕 典型的对比结论，参见曹建峰：《论互联网创新与监管之关系——基于美欧日韩对比的视角》，《信息安全与通信保密》2017 年第 8 期，第 77 页。

〔27〕 国内往往只注意到《一般数据保护条例》（679 号条例），忽略同日制定的另外两份文件（680 号指令、681 号指令）；只聚焦条例具体条文规定，忽略条例前言部分对于条例适用条件的界定；只关注条例加强个人权利保护内容，忽略条例推进合作治理的制度设计。正是被忽略的部分，体现了欧盟对于推动大数据发展的良苦用心。欧盟学者提出，“我们发现欧盟规制体系非常复杂，就数据再利用而言，一般认为欧盟法律会阻碍或者有助于再利用都不对”。Helena Ursic & Bart Custers, *Legal Barriers and Enablers to Big Data Reuse: A Critical Assessment of the Challenges for the EU Law*, 2 Eur. Data Prot. L. Rev. 209 (2016).

〔28〕 对于美国联邦贸易委员会隐私保护执法已经上升到形成“普通法”高度，以及欧盟、美国隐私法比较已经快速过时的论述，参见 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 586 (2014)。

〔29〕 Christopher Wolf, *Envisioning Privacy in the World of Big Data*, in Marc Robenberg, Julia Horwitz & Jeramie Scott (eds.), *Privacy in the Modern Age: The Search for Solutions*, The New Press, 2015, p. 204.

〔30〕 对欧美个人信息保护法律制度各自缺陷的分析，参见 Fred H. Cate, *Privacy in the Information Age*, Brookings Institution Press, 1997, p. 100。

〔31〕 英国学者指出，欧盟《个人数据保护指令》被商业组织更多看成繁文琐节和官僚主义要求，而不是帮助企业生产更好的产品。因此，尽管该指令非常严格，但只是纸面上而不是实质性被遵守。Lilian Edwards, *Coding Privacy*, 84 Chi. -Kent L. Rev. 871 (2010).

〔32〕 See Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 Seton Hall L. Rev. 996 (2017).

制度设计是否科学。探索中国个人数据治理之道，必须超越欧美两种模式的简单法规范对比，既要看到两种模式的差别，更要从两种模式中吸取有益的经验。只有这样，才能博采众长，走出一条符合我国国情的个人信息保护法治道路。

2010 年，两位美国学者发表《书本上与实践中的隐私》一文，[33] 通过对行业公认的首席隐私官的大量访谈，对美国企业过去 15 年间隐私政策的执行状况首次进行实证研究。随后，他们扩大研究范围，对四个欧盟国家（德国、法国、英国、西班牙）的企业隐私实践进行研究，大量访谈企业隐私官员、政府官员与学者，并于 2015 年出版《实践中的隐私——推动美欧企业行为》，[34] 其中很多发现让人耳目一新，获得各界广泛关注与好评。[35] 他们的重要结论包括：（1）美国与英国企业的隐私官员一般从避免给消费者预期造成损害的风险管理角度看待隐私保护，其他三个欧洲大陆国家企业的隐私官员基本从人权角度看待隐私，回避采用风险和消费者损害话语。（2）尽管在基本观念、实体法律以及执法机构等方面存在很大差异，美国与德国的企业基本以相同的方式对待隐私管理。两国隐私官员都将隐私保护当作战略问题，需要考虑的远远超出单纯遵守特定的法律规则；都将隐私当作不断演变、面向未来和依赖语境变化的社会价值，而不仅仅是个人同意与控制；都有有权并且相对自主的职业隐私官员，能够接触企业高级管理层，参与企业重要决策，并与外部利益相关者密切互动；活动很多都涉及战略性议题而不纯粹是操作层面的议题，职能远超“合规”要求，因而使企业内部的隐私决策能够与企业的战略决策、核心价值相互整合；作为企业高级雇员，隐私官员既能够自上而下指挥，也能够直接与董事会沟通；企业内部都通过分布式网络进行隐私管理，由职业隐私官员和业务单位中经过专门培训的雇员组成执行网络，从产品设计、业务开发的早期阶段就将隐私保护与业务开发紧密相联，实现双向沟通。（3）美国与德国企业的做法截然不同于法国、西班牙与英国企业的做法。西班牙与法国的企业很大程度上将隐私职能作为遵守确定的法律命令，哪怕自己怀疑做不到也要严格执行。英国企业也同样重视法律，但对于执行前景更为乐观。英国的首席隐私官在企业中的地位比美国、德国的同行要低好几个级别，能够得到的资源和参与高层决策的机会都少得多，无法在企业内部构建有效的分布式执行网络。西班牙、法国企业的隐私官员大部分都单线归属于合规或者法务部门，主要工作是满足数据登记、使用和报告等要求，隐私保护与产品、业务开发相互脱节，也缺乏执行隐私保护的分布式网络结构。（4）从法律规则实施有效性方面评价，规则越原则，企业的隐私管理实践越有效，德国与美国属于此类；规则要求越具体，执行权越集中，企业就越容易只是遵守合规要求，而不是将隐私保护内化为行动，法国、西班牙属于此类。（5）在变化的环境下，法律规则要促进企业承担更多责任，需要原则性立法和开放式监管，并辅之以能动的监管者和有效的外部利益相关方监督；搭建跨界、包容的隐私保护共同体，使政府、企业和社会的隐私专业人员能够密切互动，反过来巩固企业隐私官员在公司的地位；充分曝光隐私保护失败事例，包括数据泄露通知，加强媒体、非政府组织和公众监督，促使企业加大对隐私保护的重视和投入。两位学者的上述发现与

〔33〕 Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247 (2010).

〔34〕 Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*, MIT Press, 2015.

〔35〕 两位作者因此获得国际隐私专业人协会（IAPP）2016 年隐私领袖奖。

研究结论不仅在一定意义上打破了通常的美国与欧盟两大模式的刻板划分，也深化了对企业内部隐私保护实施机制与个人信息保护法作用机理的认识。

另一项同样基于大量访谈的实证研究发现，荷兰作为欧盟国家，其二十多年的隐私法律实施并不是通常理解的单纯政府监管，而是体现了政府部门与业界的合作治理精神。荷兰制定隐私保护法律以后，其实施都是先由各个行业协会提出企业行为规范，先后有银行、保险、直接营销等二十多个行业提出了本行业的企业行为规范，以避免政府直接监管导致的信息不对称问题；然后，各个企业行为规范需要经政府批准后才能实施，以避免纯粹的行业自律机制可能导致的力度不够、运动员与裁判员不分现象。荷兰实践中的这些做法，正好是美国政府致力于推进隐私法律制度改革的方向，美国有大量的改革计划都与荷兰的经验相似。〔36〕这样，通常理解的美国、欧盟两大模式划分，其实掩盖了各国对于合作治理方式的共同探讨。更值得关注的是，美国致力于学习的荷兰经验，在欧盟《一般数据保护条例》（下称《条例》）中得到了重视，规定了“经批准的行为规范”具有证明跨境个人信息传输合法性的法律效力，这是欧盟《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》（下称《个人数据保护指令》或《指令》）所缺乏的内容，也是欧盟在推进合作治理方面的一个重大进步。

有学者通过对爱尔兰、美国两个国家行政执法部门2011年对Facebook的执法调查案例比较研究发现，尽管两个国家个人信息保护法律规定差别很大，但由于执法部门都采用了更为有效的回应性规制方法，通过执法协议要求企业持续改进其隐私保护实践，而未采用常规的对抗式处罚方式，因此“使大洋两岸之间的明显差别难以区分”。〔37〕这样的友好型处理既能更灵活地适应技术变化带来的规制挑战，符合成本有效原则，也有利于提升真实世界的数据保护实践。

还有学者通过对德国、法国、意大利、英国四个欧盟成员国的隐私保护实证研究，发现四个国家隐私规制的共同趋势是将严格的政府执法、公共压力之下的行业自律和低水平的诉讼机制相结合，称之为“合作法治主义”模式。〔38〕这虽然不同于美国以诉讼为主的模式，但其中明显有很多相似的机制，尤其是通过执法威慑和公共压力机制促使企业更多行业自律，实现他律与自律的结合。即使法国、意大利这样的对于业界参与决策过程一直持敌视态度的国家，也在政策制定过程中纳入更多自律机制。

如果说美国一直在探讨如何构建有效的个人信息保护法律体系，欧盟则已经将制度建设付诸实施。从《个人数据保护指令》制定到《一般数据保护条例》出台，体现了既保护个人信息决定权利又促进个人信息自由流动的双重价值。这种双重价值追求，既体现在《指令》《条例》的名称中，也体现在立法结构的整体安排上，更体现在《指令》《条例》的前言、基本原则与具体规定之中。当然，鉴于《指令》制定之时移动互联网与大数据尚

〔36〕 对于荷兰法律框架结构由行业行为规范具体填补经验的介绍，以及美国国会、政府推动隐私法律制度改革的倡议，参见 Dennis D. Hirsch, *Going Dutch: Collaborative Dutch Privacy Regulation and the Lessons It Holds for U. S. Privacy Law*, 2013 Mich. St. L. Rev. 86 (2013)。

〔37〕 William McGeveran, *Friending the Privacy Regulators*, 58 Ariz. L. Rev. 961 (2016).

〔38〕 Francesca Bignami, *Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy*, 59 Am. J. Comp. L. 412 (2011).

未发展，其侧重点更多偏向个人信息保护；而《条例》的制定就必须同步考虑大数据发展的实际，为大数据发展提供法律依据，为欧盟数字经济发展留下空间。〔39〕国内解读欧盟个人信息保护法律制度，往往只强调其权利保护的一面，看到严格执行的各种要求，忽略了其促进发展的一面和制度设计中的各种平衡追求。〔40〕

从第三方独立观察的角度解读，尤其与《个人数据保护指令》比较，《一般数据保护条例》在构建多元主体参与合作治理、推动大数据发展方面的考虑，至少体现在如下三个方面：

首先，在加强对个人信息保护的同时，适应大数据时代的现实，在个人信息使用目的限制、数据留存期限等方面，尽量为大数据开发利用开辟可能的路径。比如，使用目的限制是欧盟法律的一项核心要求，《一般数据保护条例》也规定得非常严格，不允许信息控制者一揽子获得一般性同意。但是，对《条例》进行详细的分析可以发现，立法者还是故意给数据用于新的目的留下了途径。对于数据留存，《个人数据保护指令》只规定了两种方式：一是基于原始收集目的留存；二是完全匿名之后可以留存。《条例》增加了一种新的方式，允许基于统计目的，并在符合成员国各自制定的保障措施的条件下留存数据。另外，《条例》废止了过去很多情况下数据处理者需要向数据保护局“事先通知”数据处理的要求，而这一要求是《指令》构筑的核心制度。两位权威欧洲学者在比较了《条例》与《指令》在促进大数据发展方面的差别后得出结论说，“《条例》虽然并未与过去决裂，但清楚地描绘了可以用更适应大数据环境的基于使用机制来替代传统数据保护核心机制的未来路径”。〔41〕

其次，相较于《个人数据保护指令》，《一般数据保护条例》更突出强调责任原则、透明原则的地位和作用，强化信息控制者内部治理机制，调动信息控制者参与数据治理的积极性。〔42〕根据《条例》要求，信息控制者需要建立有效的技术与管理措施，包括经常进行审计、贯彻“设计即隐私”理念、执行隐私影响评估、任命数据保护官、采取与风险相适应的安全防范技术措施，事先与数据管理局咨商等，并根据环境变化及时更新，不断完善内部数据治理体系。《条例》很多新的要求都是《指令》所缺乏的，体现了立法观念上的明显进步。比如，《指令》第 18 条第 2 款并没有强制要求信息控制者设置数据保护官一职，只是倡导性规定，尽管德国、法国在实践中已经采用了这种制度。《条例》修改引入了数据保护官要求，并以充分的篇幅对其地位、职能等做了较为完备的规定，被欧盟专

〔39〕 双重价值的追求，当然也就会一直受到来自两个不同方面的攻击。从权利保护角度不够对于《一般数据保护条例》提出的批评，参见 Simon Davies, *The Data Protection Regulation: A Triumph of Pragmatism over Principle*? 2 Eur. Data Prot. L. Rev. 290 (2016)；从数据利用角度不够对于《条例》提出的批评，参见前引〔32〕，Tal Z. Zarsky 文，第 995 页。

〔40〕 国外学者对于《个人数据保护指令》权利保护视角的单向度解读，参见 Francesca Bignami & Giorgio Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 Law & Contemp. Probs. 231 (2015)。

〔41〕 Viktor Mayer-Schönberger & Yann Padova, *Regime Change? Enabling Big Data through Europe's New Data Protection Regulation*, 17 Colum. Sci. & Tech. L. Rev. 335 (2016).

〔42〕 具体论述，参见 Axel Freiherr von dem Bussche & Anna Zeiter, *Implementing the EU General Data Protection Regulation: A Business Perspective*, 2 Eur. Data Prot. L. Rev. 576 (2016)。

家普遍认为是完善信息控制者内部治理机制的核心。[43]《指令》并未规定笔名化概念或者措施,[44]《条例》引入了笔名化制度,并对笔名化和匿名化两种安全措施进行了明确区分,对笔名化提出了明确的要求,规定《条例》不适用于匿名化信息,目的是为了从源头降低信息主体的安全风险,帮助信息控制者满足法律要求,促进大数据发展。另外,《指令》未规定加密概念或措施,而《条例》明确将加密作为一项安全措施加以规定,这体现的也是“设计即隐私”的源头治理思路,鼓励企业从源头采取防范措施,有利于推动云计算发展。[45]

《一般数据保护条例》构筑合作治理最为典型的领域,当属在跨境信息传输机制上的创新。《个人数据保护指令》第25条规定向欧盟之外的第三国传输个人数据需要满足充分性要求(由欧盟委员会认定),否则不得传输。除此之外,《指令》第26条第2款还设计了变通性质的“合适合同条款”机制。一个国家虽然没有得到欧盟委员会的充分性认定,但该国之内的企业只要能签署符合欧盟要求的模范合同条款,承诺遵守保护个人数据,就可以进行跨境信息传输。实践中,企业集团或者关联企业内部跨境传输个人信息只要满足自我约束规则的要求,欧盟也认为符合充分性条件。对于美国企业,欧盟还有单独的《安全港协议》机制,美国企业只要承诺遵守相应规定,即可获得从欧盟传输个人数据的资格。[46] 这些机制设计,既弥补了一般充分性认定机制的不足,避免了《指令》实施可能导致的数据无法跨境传输窘境,也使不同企业都能找到符合自己情况的政策工具,调动其保护个人数据的积极性,带有典型的合作治理色彩。[47]《条例》在上述几种机制之外,又增加了经批准的行为规范和第三方认证具有证明跨境信息传输合法性的效力,进一步丰富了合作治理的形式,属于典型的自律与规制结合的激励性监管方式,可以更为充分地调动信息控制者主动参与的积极性。[48]

再次,通过设计强有力的外部执法威慑机制,促使信息控制者主动承担法律责任。《个人数据保护指令》过去体现的是以事前登记、信息主体决定权为核心的控制思路,缺乏有效的事后威慑手段。比如,《指令》没有明确执法协调机制,导致实践中执法标准不统一、执法管辖权模糊,增加了信息控制者的守法难度;缺乏罚款标准,将规则制定权交由各国行使,各国执行起来差别很大,普遍力度不够;[49] 没有规定个人数据泄露的通知要求,难

〔43〕 对于数据保护官在欧盟各国以及欧盟法律框架内的演变介绍,参见 Miguel Recio, *Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability*, 3 Eur. Data Prot. L. Rev. 114 (2017)。

〔44〕 成员国法律中对于笔名化的规定,参见 Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation*, 2d ed., Oxford University Press, 2007, p. 65。

〔45〕 对于加密技术在《一般数据保护条例》中法律地位不确定性的分析以及加密技术可以产生排除该条例适用效果(促进云计算)的论述,参见 Gerald Spindler & Philipp Schmechel, *Personal Data and Encryption in the European General Data Protection Regulation*, 7 J. Intell. Prop. Info. Tech. & Elec. Com. L. 163 (2016)。

〔46〕 对于欧盟这几项机制具体建立过程中的多方互动的描述,参见 Paul M. Schwartz, *The EU-U. S. Privacy Collision: A Turn to Institutions and Procedures*, 126 Harv. L. Rev. 1979 (2013)。

〔47〕 对于 Schrems 案后,这些不同机制均可能遇到欧盟法院审查挑战以及判决执行方面会遇到的各种障碍,参见 Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, 18 German L. J. 881 (2017)。

〔48〕 学术界理论讨论,参见 Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 J. L. & Pol'y for Info. Soc'y. 355 (2011)。

〔49〕 对欧盟法律过去缺乏行政处罚尤其是罚款缺陷的分析,参见 Sebastian J. Golla, *Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR*, 8 J. Intell. Prop. Info. Tech. & Elec. Com. L. 70 (2017)。

以通过公开与社会监督机制形成有效压力。正因为如此，《指令》虽然事前要求很多，但一旦信息控制者违反规定，后果可能并不严重甚至流于形式，这影响了《指令》的权威性和有效性。针对威慑不强这一突出问题，《一般数据保护条例》进行了全面改进，其主要措施包括：确立牵头数据管理局，加强各国执法合作，避免不同国家多头执法导致的执法标准不统一；〔50〕统一设立最高罚款上限为 2000 万欧元或者信息控制者上一年度全球营业额 4% 的罚款标准，大幅提高罚款的幅度；增加个人信息泄露后分别通知数据管理局和信息主体的义务，建立有效外部威慑机制。〔51〕《条例》的这些新措施，明显与美国的很多执法威慑机制类似，既消弭了欧美过去的很多制度设计差异，也有利于通过强有力的外部威慑机制促使信息控制者更好承担数据治理责任。

相较于《个人数据保护指令》，《一般数据保护条例》的整体制度设计思路更清晰、规定更翔实，充分体现了通过更有效的内部治理、更强的外部威慑，促使信息控制者主动承担更多责任的立法意图，符合激励监管的基本原理。如果说法律规定是外在的表现形式，那么追求法律的有效实施机制就是内在动力，两者之间是器与道、形与神的关系。后发国家如果只看到美欧法律规定的表面差别，看不到背后的作用机理，就很难从其经验与教训中获得任何有益的启示。

三、培育信息控制者的内部治理机制

发展中国家不同于欧美发达国家，不论是基本权利保护还是消费者预期保护，在信息控制者的行为序列中可能都还难以达到同样的高度。制定个人信息保护法，首先要找到信息控制者最基本的激励，并围绕核心激励设计相关的制度。对于所有信息控制者而言，最基本的需求肯定都是发展与安全。发展是目标，安全是实现目标的保障；缺乏安全保障，不可能有发展。由于技术水平的差距，发展中国家面临的安全挑战比发达国家要大得多。从安全防范角度切入，在发展中国家应该是最容易为信息控制者接受的解决方案。

安永第 19 届《全球信息安全调查报告》采访了 1735 名首席管理人员、信息安全与 IT 高管或经理，他们代表了众多全球规模最大且最知名的企业。2017 年 9 月发布的调查报告显示，在过去两年中，87% 的公司董事会成员和企业高管都表示对其公司层面的网络安全缺乏信心；44% 的企业没有安全运营中心，64% 的企业没有或只有非正规的威胁情报计划，55% 的企业没有或只有非正规的漏洞识别能力；62% 的企业在经历了看似无害的安全事件后，并不会增加其网络安全支出；部分企业怀疑自身是否有能力继续识别网络中的可疑流量（49%）、追踪数据的访问者（44%）或发现潜藏的未知“零日漏洞”攻击（40%）；89% 的企业不去评估每次重大事件所带来的财务影响，而在 2016 年遭受过网络安全事件的企业中，有近半数（49%）对该网络事件造成或可能带来的经济损失并不了解。〔52〕另据针

〔50〕 相关介绍，参见 Hielke Hijmans, *The DPAs and Their Cooperation: How Far Are We in Making Enforcement of Data Protection Law More European?* 2 Eur. Data Prot. L. Rev. 362 (2016)。

〔51〕 相关介绍，参见 Jasmien Cisar and Julien Debussche, *Novel EU Legal Requirements in Big Data Security: Big Data-Big Security Headaches?* 8 J. Intell. Prop. Info. Tech. & Elec. Com. L. 84 (2017)。

〔52〕 安永：《网络弹性之路：感知、抵御、应对——安永第 19 届全球信息安全调查报告》(2017 年)，第 9 页。

对13个国家与地区419家公司的调研，2017年每家公司数据泄露的平均成本为362万美元，每人次个人数据泄露的平均成本为141美元；〔53〕诸如南非、印度等发展中国家，在未来24个月内最有可能发生人次超过1万以上的实质性数据泄露事件，而德国、加拿大发生这种事件的概率最低。〔54〕

从国内外近年来屡屡发生的各种数据泄露案例来看，信息控制者面临的安全挑战压力是现实的，也是巨大的。个人数据泄露会造成声誉、法律责任承担与客户流失等影响，而随着竞争加剧，“隐私成为品牌”，〔55〕有效保护个人信息会成为市场主体的核心竞争力，价值会逐步外溢，成为无形资产。

对于信息控制者而言，从信息安全角度来保护个人信息，本应该是顺理成章的事，个别行业领先企业也已经自发在进行相关的内部治理机制探索。但是，过去对信息安全约定俗成的理解，并不包括个人信息安全或者隐私保护。〔56〕基于这种背景，1994年制定的《计算机信息系统安全保护条例》，目的是为了保护计算机信息系统的安全，保障计算机及其相关的和配套的设备、设施（含网络）及其运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。2004年公安部、国家保密局、国家密码管理委员会办公室、国务院信息化工作办公室印发《关于信息安全等级保护工作的实施意见》，2007年四部门又印发《信息安全等级保护管理办法》，完整建立了我国的信息安全等级保护制度。随后，国家通过陆续制定统一的信息安全等级保护管理规范和技术标准，对信息系统分等级实行安全保护。在信息安全等级保护制度中，保护的对象主要是重要信息和信息系统，在上述文件和《信息安全技术·信息系统安全等级保护基本要求》（GB/T 22239－2008）以及该国家标准所指引的“共同构成了信息系统安全等级保护的相关配套标准”中，〔57〕均缺乏关于个人信息保护的规定，使个人信息保护一直游离于信息安全等级保护制度之外。〔58〕这样，在传统的信息安全观念下，信息控制者长期考虑的只是计算机系统安全或者运行安全，〔59〕力图通过权限管理、病毒查杀、设立防火墙、VPN、入侵检测等管

〔53〕 See Ponemon Institute, *2017 Cost of Data Breach Study: Global Overview*, 1 (June 2017).

〔54〕 同上引报告，第5页。

〔55〕 参见前引〔31〕，Lilian Edwards文，第872页。

〔56〕 几位权威专家在对信息安全的全面论述中，根本没有提到个人信息或隐私概念。参见沈昌祥等：《信息安全综述》，《中国科学》2010年第2期，第129页。

〔57〕 包括《信息安全技术·信息系统安全等级保护定级指南》（GB/T 22240－2008）、《信息安全技术·信息系统通用安全技术要求》（GB/T20271－2006）、《信息安全技术·网络基础安全技术要求》（GB/T20270－2006）、《信息安全技术·操作系统安全技术要求》（GB/T20272－2006）、《信息安全技术·数据库管理系统安全技术要求》（GB/T20273－2006）、《信息安全技术·服务器安全技术要求》（GB/T 21028－2007）、《信息安全技术·终端计算机系统安全等级技术要求》（GA/T671－2006）、《信息安全技术·信息系统安全管理要求》（GB/T20269－2006）、《信息安全技术·信息系统安全工程管理要求》（GB/T20282－2006）、《信息安全技术·信息系统安全等级保护实施指南》（GB/T 25058－2010）。

〔58〕 一直到2012年由工业和信息化部推动制定了《信息安全技术·公共及商用服务信息系统个人信息保护指南》（GB/Z 28828－2012）。由于缺乏上位法支撑，该指导性技术标准实践中的影响力非常有限，并且该标准对个人信息管理者内部治理机制的要求非常简单、原则。

〔59〕 企业对于信息安全问题的通常理解，参见游湧：《证券公司交易系统信息安全保障体系的构建研究》，《科技创业月刊》2011年第13期，第50页；罗天保：《汽车公司网络安全方案研究》，《现代计算机》2008年第8期，第103页；田波、吴倩、甄浩：《航空公司信息安全管理系统的构建与安全保障体系研究》，《情报科学》2011年第9期，第1392页；陈春霖、屠正伟、郭靓：《国家电网公司网络与信息安全态势感知的实践》，《电力信息与通信技术》2017年第6期，第3页。

理与技术措施，防止系统被攻击和瘫痪，未能将个人信息保护纳入安全框架内一并予以考虑，导致信息安全管理与个人信息保护存在长期的相互脱节现象。〔60〕

近年来国家明显加大了个人信息保护的立法进程，2009 年侵权责任法首次在法律中确立了隐私权的法律地位。同年，刑法修正案（七）设立了出售、非法提供公民个人信息罪与非法获取公民个人信息罪两个罪名。2012 年《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》，第一次从法律上界定了个人信息的内涵和范围，也是我国法律第一次对个人信息保护实体内容进行较为系统的规定。2013 年修订的消费者权益保护法，明确将个人信息得到保护的权利列为消费者的一项基本权利，全面突出强调了消费者个人信息保护方面的内容。2015 年刑法修正案（九）对刑法修正案（七）的规定予以进一步完善，将两个罪名合并为侵犯公民个人信息罪一个罪名，还增设了拒不履行信息网络安全管理义务罪。2016 年制定的网络安全法是迄今为止对个人信息保护规定最为全面的立法，它明确要求网络运营者建立健全用户信息保护制度。2017 年民法总则第 111 条规定，自然人的个人信息受法律保护。

由于缺乏专门的个人信息保护法，我国个人信息保护相关立法目前普遍存在两个突出问题：一是规定过于原则，往往只是一个概念或者一个具体要求，通常是禁止性要求，〔61〕缺乏系统的整体制度设计，即使网络安全法对于个人信息保护也都只是一些非常原则性的规定；〔62〕二是普遍重责任追究，尤其是刑事责任追究，轻过程规范，轻综合治理。只要发生不利结果，就责任很重，甚至可以直接刑罚制裁，而信息控制者究竟应该履行哪些法律义务则缺乏规定。〔63〕比如，按照《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》，对于侵犯公民个人信息罪“情节严重”采用了十种不同的判定标准，符合标准之一就可以定罪。〔64〕这样，几乎所有侵犯公民个人信息行为都可能直接触发刑事责任，完全可以替代任何行政执法机制，〔65〕更不需要内部治理机制

〔60〕 安全管理通常是安全管理部门或者信息中心的职责，个人信息保护通常是法务或者合规部门的职责。

〔61〕 有学者指出，“措施性的规定很可能造成管理对象仅仅止步于合规，而缺乏动力去采用国家标准和行业标准要求之外的安全措施”。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》，《环球法律评论》2016 年第 4 期，第 30 页。

〔62〕 2017 年 12 月 29 日发布的《信息安全技术·个人信息安全规范》（GB/T 35273－2017）首次较全面地对数据控制者的行为与组织提出了要求，但由于其推荐性标准的定位，法律效力有限。并且，由于网络安全法等上位法规定本身非常原则，该标准的一些规定面临缺乏上位法支撑的问题。

〔63〕 有学者将目前这种状态归纳为“刑先民后”，并指出“在缺乏其他法律尤其是民事法律提供的最基础保护的前提下，刑法势必独木难支”。于志刚：《“公民个人信息”的权利属性与刑法保护思路》，《浙江社会科学》2017 年第 10 期，第 11 页。

〔64〕 该司法解释第 5 条规定，非法获取、出售或者提供公民个人信息，具有下列情形之一的，应当认定为刑法第 253 条之一规定的“情节严重”：（1）出售或者提供行踪轨迹信息，被他人用于犯罪的；（2）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；（3）非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息 50 条以上的；（4）非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息 500 条以上的；（5）非法获取、出售或者提供第三项、第四项规定以外的公民个人信息 5000 条以上的；（6）数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的；（7）违法所得 5000 元以上的；（8）将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，数量或者数额达到第三项至第七项规定标准一半以上的；（9）曾因侵犯公民个人信息受过刑事处罚或者 2 年内受过行政处罚，又非法获取、出售或者提供公民个人信息的；（10）其他情节严重的情形。

〔65〕 有刑法学者明确指出，对于侵犯公民个人信息行为，“我国刑法先于行政法、民事法亮剑”。但是，“综合我国法律传统与他国经验，行政处罚应是惩治侵犯公民个人信息行为的最主要法律制裁手段”。卢建平、常秀娇：《我国侵犯公民个人信息犯罪的治理》，《法律适用》2013 年第 4 期，第 27 页。

配合。〔66〕结果，近年来的密集立法不但未能解决信息控制者内部信息安全与个人信息保护脱节问题，还导致外部法律要求与信息控制者内部治理机制脱节、刑法制裁与其他法律手段脱节、责任规范与行为规范脱节等现象，呈现典型的命令控制式立法特点。刑事责任规定虽然看似严格，实际效果却非常有限。〔67〕随着大数据发展，一些市场主体已经意识到个人信息保护的重要性，并进行相关的主动探索，但囿于内部体制分割，加之法律规定导致的各种脱节现象，始终无法破解“两张皮”“多张皮”问题症结。

个人信息保护法要做的，就是针对上述各种脱节现象，借鉴近年来国际社会的实践经验与国内行业领先企业的有益探索，以培育信息控制者内部治理机制为目标，将个人信息保护要求嵌入整体信息安全防范体系中，明确各个环节的相关法律义务和组织要求，完善多元参与与互动机制，实现法律规范的外在要求与信息控制者的内在需要激励相容，达到既保护个人信息安全又强化信息控制者的安全防范能力的双赢结果。这就涉及观念更新、组织与流程再造、行为方式调整等各个方面，是一项系统工程，需要进行全面的制度设计。〔68〕

首先，需要更新信息安全观念，〔69〕走出传统的运行安全、系统安全的纯技术路径依赖，适应大数据时代的特点，确立数据安全观念，把数据当做核心资产，确立用户个人信息至上的基本价值观，培育保护个人信息就是维护核心竞争力的意识，积极主动承担个人信息保护责任。尽管观念更新仅仅依靠立法不可能完全解决，但通过个人信息保护法明确相应的法律义务与要求，加大违法行为的责任承担，一定有助于改变长期积重难返的各种认识模糊问题。

其次，结构决定功能，观念明确以后，有效的组织结构就是基础。如果能够从结构上构筑信息控制者积极主动作为的组织体系，就完全有可能改变其行为方式，使个人信息保护成为其内生机制的一部分。个人信息保护法应明确要求信息控制者指定或者设立专门机构或具有相应资质的专门人员（数据保护官），负责本单位个人信息保护日常工作，包括参与涉及个人信息保护所有重大决策的个人信息影响风险评估、负责拟定个人信息保护政策、与相关个人信息保护主管部门或行业自律组织联络、组织个人信息保护安全培训、接受信息主体的投诉等。数据保护官应独立履行职责，享有任职保障，并直接向本单位最高管理层负责，使最高决策层能够直接过问个人信息保护问题。要破解前面提到的各种脱节现象，务必从组织体系上实现个人信息保护与信息安全管理、安全管理与业务发展相互融合。安全管理一定要能够分布式延伸到每一条业务线，与业务团队实现无缝对接，既实现安全管

〔66〕 对于“刑法被作为个人信息保护的廉价工具，刑法的功能定位也被模糊化”的具体分析，参见田诗媛：《大数据时代个人信息保护的刑法边界——以侵犯公民个人信息罪为例》，《江西警察学院学报》2017 年第 2 期，第 78 页。

〔67〕 有学者对我国象征性刑法立法的消极影响进行了非常有见地的分析，并指出“我国网络犯罪的刑罚法规缺乏法律本该具有的实质效果”。刘艳红：《象征性立法对刑法功能的损害——二十年来中国刑事立法总评》，《政治与法律》2017 年第 3 期，第 43 页。

〔68〕 2003 年，原国务院信息化工作办公室委托笔者牵头起草了个人信息保护法（专家建议稿）。2017 年 3 月，国家互联网信息办公室政策法规局委托笔者牵头研究并提供一份个人信息保护法建议稿。后者较前者改进最大的地方就在于，在培育内部治理机制方面设计的许多制度都是过去缺乏的，是新的制度。参见周汉华：《中华人民共和国个人信息保护法（专家建议稿）及立法研究报告》，法律出版社 2006 年版。

〔69〕 国内外对于信息安全、网络安全、网络空间安全概念的一般使用辨析，参见王世伟：《论信息安全、网络安全、网络空间安全》，《中国图书馆学报》2015 年第 2 期，第 72 页；王世伟、曹磊、罗天雨：《再论信息安全、网络安全、网络空间安全》，《中国图书馆学报》2016 年第 5 期，第 4 页。

理政策的有效触达，又全方位为业务发展保驾护航，有效解决“两张皮”“多张皮”现象。从国内行业领先企业的探索实践看，〔70〕尤其在制度建设的过渡阶段，由于安全部门的地位更受重视，与业务线融合更好，由安全部门从企业数据安全角度负责个人信息保护，可能比法务部门从合规角度负责个人信息保护更为有效，更有利于迅速推进各种融合。当然，由于不同信息控制者的实际情况不一样，个人信息保护法不宜“一刀切”地介入信息控制者内部职能划分，但推进融合的大方向显然是非常明确的。不同的信息控制者应该根据本身实际情况，采取最有效的推进融合的组织形式。

再次，改变过去合规与业务流程设计相互分离、就合规谈合规的传统做法，从业务流程设计开始就将个人信息保护要求嵌入产品与服务之中，体现“设计即隐私”理念，实现个人信息保护全流程覆盖、全业务贯通的行为方式转变。在大数据环境下，不从源头设计个人信息保护，无法真正防范信息安全风险，〔71〕这是推进组织融合的出发点和目的，也是行为方式转变的核心。为此，个人信息保护法需要设计一些重要的制度，主要包括：（1）在网络安全法确立的合法、正当、必要原则之外，明确将责任原则也确立为个人信息保护的一项基本原则，促使信息控制者积极履行责任，防范风险发生。（2）信息控制者在采用涉及处理个人信息的新措施、新技术、新应用之前，应进行个人信息影响风险评估，并采取相应的安全措施，预防风险发生。评估可能存在高风险，技术上或者经济上无法有效化解这种风险的，应事先咨询个人信息保护主管部门的意见，建立有效的咨询协商机制，共同解决问题。（3）应鼓励个人信息控制者采用笔名化、加密保护、匿名化等方式处理个人信息，从源头防范个人信息泄露、被滥用等风险，并明确规定经匿名化处理的信息不适用个人信息保护法。这样，既可以弥补网络安全法第 42 条对于脱敏信息的规定法律效果不明确的弊端，有利于推动大数据开发利用，也与欧盟及其他国家对于匿名化信息的规定保持一致。（4）应要求信息控制者定期主动对信息系统个人信息安全进行检测评估，提高风险防范能力和安全事件应急处置能力。（5）应平衡个人信息保护与大数据开发利用以及其他社会公共利益的关系，明确将为统计分析、档案管理与新闻报道、学术研究、艺术表达、文学创作等目的处理个人信息的活动，根据具体情况豁免或者克减适用个人信息保护法的某些规定，具体办法由国务院个人信息保护主管部门会同相关部门制定，为信息控制者推动大数据开发利用提供法律接口。（6）对于跨境个人信息传输，除设计类似于欧盟的“充分性”认定机制，以国家为对象采取对等措施以外，还应设计多元的补充认定机制，包括经核准的标准个人信息保护合同条款、企业自我约束规则、行为规范，以及获得合法备案的个人信息保护可信标志或认证标志等。以信息控制者为适用对象，分别适用于不同的场景，解决不同的实际问题。只有这样，才能调动信息控制者参与个人信息保护的积极性，促进正常国际经贸往来。

近年来国内外发生的各种个人信息安全事件，如 CSDN 遭受攻击、12306 网站信息泄露、徐玉玉被诈骗致死案、支付宝年度账单事件、Yahoo 邮箱泄露案、Equifax 征信信息窃取案等，根源大多是信息控制者内部安全防范环节出现了问题，尤其是疏于防范、遭黑客攻

〔70〕 阿里巴巴推出的数据安全能力成熟度模型（DSMM）获得了广泛的关注，已被纳入国家标准研究项目并对外公开征求意见。

〔71〕 See Ira S. Rubinstein, *Regulating Privacy by Design*, 26 Berkeley Tech. L. J. 1410 (2011).

击、内部人非法提供、新业务开发与安全保护脱节等。只要能够构建有效运转的内部治理机制，将个人数据安全纳入整体安全防范体系，绝大部分类似事件都应该能预防、避免。

四、构筑有效的外部执法威慑

发育激励相容的内生机制，核心在信息控制者的自律。但是，在利用与保护个人数据激励失衡的大背景下，不论是合作规制理论还是各国个人信息保护实践均证明，完全依靠自律机制并不能形成有效的激励约束。〔72〕只要个人数据能够带来利益，这种现象就难以改变。制定个人信息保护法的国家，一项重要的立法任务就是构建有效的外部执法威慑，促使信息控制者积极履行法律责任，并对违法处理个人信息的行为予以制裁。美国虽然没有制定统一的个人信息保护法，但有着其他国家无法比拟的强大的外部执法威慑机制，能够约束信息控制者的行为。美国宪法、联邦法律、州法对于个人信息都有相应的保护规定，只是联邦层面缺乏一部统一的适用于市场主体的个人信息保护法。美国联邦贸易委员会、各州总检察长、民事（集团）诉讼、国会监督与媒体监督及社会监督等机制丝毫不亚于欧盟国家个人信息管理局的执法力度。对于某些特殊领域个人信息的保护，如征信信息、未成年人信息、金融信息、健康信息、电子通讯等，美国还有专门联邦立法及相应的执法机制，保护力度更大。〔73〕以美国经验说明后发国家不需要制定个人信息保护法，没有任何说服力。

由于缺少统一的个人信息保护法，我国在外部执法威慑机制构建方面除了前述的刑法机制替代其他执法机制、信息控制者实体行为规范缺位以外，实践中还导致国家网络安全保护与个人信息保护错位现象，进一步加剧规则适用的紊乱和系统性失灵。

在国家信息网络专项立法规划中，信息网络立法是分层规划、分层设计的，网络安全法与个人信息保护法是两部独立的立法，各自有其立法目的、原则、任务与制度。网络安全是国家安全的重要组成部分，事关国家根本利益，不容半点妥协，没有网络安全就没有国家安全。个人信息权是个人权利的组成部分，权利有相对性，需要依法行使，同时承担义务，权利与权利之间出现冲突需要协调，〔74〕为了国家安全与公共利益可能还需要对权利进行必要的限制或克减。〔75〕正因为国家安全与个人权利的这种性质与位阶差别，在各国立法与国际条约中，如《公民权利和政治权利国际公约》第4条、《欧洲人权公约》第15条等，均明确国家安全是更高价值，予以最高等级的保护；而个人信息权利的行使不但要以法律的规定为前提，还要受到国家安全与公共利益的限制。〔76〕

---

〔72〕 对于自律机制根本缺陷的分析，参见 Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1681 (1999)。

〔73〕 对于美国各州检察长隐私保护领域发挥重要作用的实证研究，参见 Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747 (2016)。

〔74〕 对权利冲突现象以及权利平等保护的系统论述，参见刘作翔：《权利冲突的几个理论问题》，《中国法学》2002年第2期，第56页。

〔75〕 对于国际上不可克减权利的研究，参见龚刃韧：《不可克减的权利与习惯法规则》，《环球法律评论》2010年第1期，第5页。

〔76〕 另外，《欧洲人权公约》第8条规定每个人都享有私人和家庭生活受到尊重的权利，公权力不得干预，但为了国家安全、公共安全与国家的经济福利而依法进行的必要干预除外。欧盟《一般数据保护条例》《个人数据保护指令》在明确个人信息权属于一项基本人权的同时，均申明“个人信息权不是一项绝对的权利”。

由于网络安全法制定的时候，个人信息保护法尚未被纳入国家正式立法计划，因此该法自然承担了部分个人信息保护法的立法任务，集中反映在第四章的相关规定中。用立法工作部门的话来说，该法“进一步完善了个人信息保护规范，这些规范与国际通行规则是基本一致的”。〔77〕也就是说，网络安全法同时承担了双重任务：一是保护国家网络安全，这是该法的主要任务；二是保护个人信息安全，这是该法的附带任务。如果能够把握法律关系的本质，分别适用不同的判断标准与制度，本来应该不会出现不同任务之间的错位问题。

但是，由于个人信息保护法缺位，加之其他各种复杂的原因，实践中已经出现的问题是，执法部门有时候会将双重任务混合，就高不就低，将保护国家网络安全的标准适用到个人信息保护领域，导致法律关系出现错位和紊乱。最为典型的事例当属数据本地化要求。在网络安全法中，由于关键信息基础设施的特殊地位，运营者掌握的个人信息和重要数据直接事关国家安全，必须以本地化为原则，确需出境的，依法进行国家安全评估后才能出境。相反，对于一般网络运营者或者信息控制者而言，其个人信息出境只涉及个人权利保护，数据出境可以有多种制度安排，如基于信息主体的同意、第三国满足充分性认定要求、维护第三人的重要利益、满足其他替代认定机制等。一个非常重要的差别是，国家安全评估的对象是相关个人信息和重要数据是否涉及国家安全、是否适合出境，而跨境个人信息传输的评估对象是接受个人信息的第三方是否能够有效保护个人信息，评估的对象与标准都截然不同。如果将国家网络安全标准适用于个人信息保护，势必混淆评估对象和法律关系，抬高保护门槛，不利于正常的国际经贸交流。〔78〕已经发布的《信息安全技术·个人信息安全规范》（GB/T 35273－2017）8.7（个人信息跨境传输要求）规定，“在中华人民共和国境内运营中收集和产生的个人信息向境外提供的，个人信息控制者应当按照国家网信部门会同国务院有关部门制定的办法和相关标准进行安全评估，并符合其要求”。这一规定是典型的以国家安全评估代替个人信息跨境传输保护水平评估，混淆了两项根本不同的制度，强制推行会导致各种意想不到的严重后果，也不利于真正保护国家网络安全。

可见，加快出台个人信息保护法，科学厘清不同制度的边界，不仅能解决刑法规范替代其他执法机制、信息控制者行为规范缺失等问题，也能理顺个人信息保护法与网络安全法的关系，解决好外部执法威慑机制越位、缺位与错位并存的三大现实问题，形成有效的立法结构，推动大数据利用与个人信息保护的协调发展。

构筑有效的外部执法威慑，并不是为了执法而执法，更不是为了增加信息控制者的负担，而是为了推动信息控制者形成有效的内生治理机制。为此，个人信息保护法应从明确行为规范、加大违法成本、增强信息披露、提高违法行为被发现的可能性、完善行政处罚

〔77〕 杨合庆：《中华人民共和国网络安全法释义》，中国民主法制出版社 2017 年版，第 101 页。

〔78〕 国家互联网信息办公室 2017 年 4 月 11 日发布的《个人信息和重要数据出境安全评估办法（征求意见稿）》第 2 条规定，“网络运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据，应当在境内存储。因业务需要，确需向境外提供的，应当按照本办法进行安全评估”。该征求意见稿一是明显扩大了网络安全法第 37 条对于“关键信息基础设施的运营者”的界定范围，引发很多批评；二是将国家安全评估适用于非国家安全相关的一般网络运营者，导致与国际通行规则完全不一致的结果。学术界批评意见，参见刘金瑞：《关于〈个人信息和重要数据出境安全评估办法（征求意见稿）〉的意见建议》，《信息安全与通信保密》2017 年第 6 期，第 72 页。

与刑事责任的衔接、推进合作治理等多角度，构筑有效威慑机制，构筑“胡萝卜 + 大棒”的激励约束格局，促使个人信息保护要求能够真正被信息控制者严格执行。如下几个方面的制度设计不可或缺：

首先，与培育内部治理机制相衔接，扩大责任原则的边界，通过行业领先者的标杆作用提升行业整体保护水平。个人信息保护法需要明确规定，信息控制者依法向第三方提供、转移、共享或者跨境传输其合法控制的个人信息的，应保证第三方能够履行同等个人信息保护法律义务，确保个人信息全流程安全，保证责任原则的全面实现。这将有利于提升行业整体保护水平，避免木桶效应，改变违法成本低、守法成本高的逆向选择问题。

其次，确立并贯彻落实透明原则，以公开透明促内部治理结构发挥作用。个人信息处理过程公开透明，是信息控制者形成内生机制的重要外部条件和运行保障，能有效弥补合法、正当、必要等原则的不足。〔79〕个人信息保护法应明确规定，发生个人信息泄露的，信息控制者应当在知情后及时——最迟不超过 72 小时——向个人信息保护主管部门报告，除非泄露不会对信息主体的合法权利产生风险。不能在 72 小时内报告的，应说明理由。第三方发生个人信息泄露的，除向个人信息保护主管部门报告外，还应同时通知信息控制者。个人信息泄露可能对信息主体权利产生高风险的，信息控制者应以清晰、简洁的语言，尽快通知信息主体。

再次，明确信息控制者行为底线，完善行政执法手段和合作治理机制，及时发现违法行为。个人信息保护法应明确规定：信息控制者不得以不公平条件或者“一揽子协议”方式，强制或者变相强制信息主体授权对个人信息的收集；对于特殊类型个人信息（如基因、生物、健康、种族、信仰、征信等），实行特殊保护，禁止或者限制信息控制者采集，构筑个人信息安全防控底线；信息控制者采用预测性识别技术，应采用公平的数学或统计学方法，禁止基于种族、民族、政治观点、宗教或者信仰、基因或者健康状态等差别对信息主体进行歧视；处理基因数据、生物数据、健康状况数据等敏感数据，以个人信息处理为主要业务，处理个人征信数据或者处理刑事裁判数据等，须经政府个人信息保护主管部门行政许可。个人信息保护法应推动形成内外互动的职业共同体和多方交流平台，包括制定行业行为规范等，不断将外部压力传导到信息控制者内部。个人信息保护法应着力完善行政执法手段，规定个人信息保护主管部门可以约谈信息控制者的高级管理人员，要求就个人信息保护重大事项作出说明，提示个人信息保护面临的风险，要求及时进行相应整改，加强过程监管和协商治理。信息控制者违法进行个人信息处理的，政府个人信息保护主管部门应当有多种方式的管理手段，包括责令限期改正，责令暂停个人信息处理，责令消除影响、赔礼道歉，责令停止使用个人信息文件、个人信息系统，责令提供个人信息，责令更正、停止使用、限制处理或者删除个人信息，责令销毁个人信息文件、个人信息系统，责令停止跨境信息传输，警告并发布风险提示，罚款，吊销个人信息处理登记证或许可证等。对于严重违法行为，个人信息保护法应提高行政处罚标准，引入累犯加罚，按照违法处理个人信息条数处以罚款等。

〔79〕 网络安全法只规定了合法、正当、必要三项基本原则，并在第 42 条第 2 款规定，“在发生或者可能发生”个人信息泄露的情况时，都要按照规定及时告知用户并向有关主管部门报告。由于数据风险无时不在，规定可能发生泄露也要通知，不符合数据保护的实际。

最后，借鉴消费者权益保护法修改经验，加大民事责任追究力度，解决个人信息被滥用后民事维权成本高、收益低问题，〔80〕调动信息主体依法维权的积极性。个人信息保护法应规定：信息主体认为信息控制者的个人信息处理行为违反法律的规定，侵犯其合法权益导致其人身、财产或者精神损害的，可以依法直接向人民法院提起民事诉讼，要求停止侵害，消除影响，赔偿损失，包括精神损害赔偿；具备条件的社会组织，就损害信息主体合法权益的行为，支持受损害的信息主体提起诉讼或者依法提起诉讼；信息控制者的信息处理行为违反法律的规定，给信息主体的人身、财产或者精神合法权益造成损害的，应依法承担赔偿责任；赔偿的金额不足 500 元的，为 500 元；法律另有规定的，依照其规定。

五、把握循序渐进的推进节奏

培育信息控制者内部治理机制与构筑有效的外部执法威慑，只是信息控制者与管理者两个主体之间的单维度关系，属于监管范畴的制度构建。要实现大数据利用与个人信息保护之间的协调发展，肯定不能遗漏信息主体及其权利行使，这就涉及信息主体、信息控制者、管理者三者之间的多维治理结构。缺乏信息主体参与，缺乏完整的治理结构支撑，不可能出现激励相容的结果，大数据发展与个人信息保护不可能实现持久平衡。当然，一旦引入多维视角，问题就会复杂得多。美欧两种模式之间的真正差别，其实在于究竟是在多维还是在单维中考虑个人信息保护。欧盟从一开始就需要处理好基本权利保护与信息自由流动不同价值之间的关系，注定了要在多维视角中解决问题，因此一直面临很大的平衡压力。但在长期努力之下，其基本理念与制度已经被其他国家普遍接纳。美国一直回避基本权利话语，仅从消费者风险防范单维度考虑个人信息安全，处理起来更为简单。美国在国际上能够特立独行，一是因为美国商界对于创新的重视和对政府监管的怀疑；二是国内强有力的执法机制，能够有效规范市场主体的行为；三是在国际上具有霸权地位，可以靠实力推行自己的一套价值观。美国所具有的这些条件其他国家大多难以完全具备，其做法也难以为其他国家所照搬。但是，随着大数据带来的个人信息安全关切日益上升，美国也一直面临越来越大的国内外压力，要求更重视消费者权利，让消费者有权控制自己的信息。〔81〕奥巴马政府 2012 年首次发布消费者隐私权利法案白皮书，2015 年直接以法案形式提出完整的立法建议，都是希望以消费者控制为核心理念来完善制度，赋予消费者控制哪些个人信息可以被收集以及这些信息如何使用的权利。〔82〕尽管这些建议尚未能付诸实践，但已经反映了制度构建上多维视角的重要性，欧盟长期面临的双重价值平衡问题迟早也会在美国出现。

我国制定个人信息保护法，不能够也不应该回避权利话语。这主要是因为：首先，要

〔80〕 对于典型民事诉讼案件中原告胜诉难以及经济损失证明难的介绍，参见中国青年政治学院互联网法治研究中心、封面智库：《中国个人信息安全和隐私保护报告》（2016 年 11 月），第 26 页。

〔81〕 对于美国法律难以保护消费者隐私以及借鉴欧盟经验改革的论述，参见 Michael D. Simpson, *All Your Data are Belong to Us: Consumer Data Breach Rights and Remedies in an Electronic Exchange Economy*, 87 U. Colo. L. Rev. 669 (2016)。

〔82〕 The White House, *Consumer Data Privacy in A Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 4 J. of Pri. and Conf. 10 (2012).

继续参与国际经贸交往，我们只能构建国际通行的多维话语体系与个人信息保护法律制度，否则很有可能被排斥在国际规则体系之外。其次，近年来的国内相关立法已经在个人信息权利保护上迈出重要的步伐，包括民法总则第111条在民事权利部分明确规定保护个人信息，2013年消费者权益保护法修改后纳入了后悔权和个人信息权等新类型权利，《征信业管理条例》系统构建了信息主体对于个人征信信息的控制制度，网络安全法在回避使用权利概念的同时实际上部分确立了包括被遗忘权在内的新型权利的法律地位。随着社会的发展，不论是私法性质还是公法性质的权利，权利的种类、范围等都在不断扩大之中，〔83〕个人信息保护法要顺应大数据发展历史潮流，承担推进个人信息保护的历史责任。〔84〕最后，其实也是最重要的理由在于，随着大数据广泛使用，个人信息面临的威胁也同步加大，公众对于个人信息安全的需求和意识会越来越强烈，法律必须予以回应。

2014年，中国消费者协会的个人信息保护状况调查发现，约三分之二受访者在过去一年内个人信息曾被泄露或窃取。受访者中，认为“服务商未经本人同意，暗自收集个人信息”是消费者个人信息泄露的最主要途径，占比达64.08%。〔85〕中国信息通信研究院的一项实证调查也发现，近80%的用户认为隐私泄露严重，防不胜防；并且，用户维权意识提升，认为企业“不告知收集”和“非法买卖个人信息”是突出问题。〔86〕另一项权威数据显示，2016年遭遇过网络安全事件的用户占比达到整体网民的70.5%，其中网上诈骗是网民遇到的首要网络安全问题，39.1%的网民曾遇到过这类安全事件。〔87〕公安部刑侦局有关负责人几年前就表示，侵害公民个人信息犯罪是多种下游犯罪的源头，社会危害巨大，除引发电信、网络诈骗等各种新型犯罪外，还与绑架、敲诈勒索、暴力追债等黑恶犯罪合流。〔88〕2016年底徐玉玉案之后，公民个人信息泄露导致的生命财产威胁引起社会各界广泛关注。在个人信息面临各种严峻挑战、公众信息安全意识逐步提升的大背景下，个人信息保护法如果不确立公众维护自己权利的制度，不能满足公众的最基本安全需求，公众一定会用实际行动（包括用脚投票）来维护自己的信息安全，动摇大数据发展的基石，结果只会导致信息控制者、管理者、信息主体的双输或者多输结果。

因此，个人信息保护法应该在近几年各项立法的基础上，借鉴国际社会成功经验，包括美国与欧盟的经验，以全面构建个人数据治理体系为原则，以防范个人信息安全风险为目标，明确引入公法意义上的个人信息控制权概念，〔89〕并在收集、使用、转移、存储、跨境传输、销毁、查询、更正等个人信息处理的全过程，明确信息主体的知情权、同意权、

〔83〕 参见梁慧星：《民法总论》，法律出版社2007年版，第77页；周汉华：《行政许可法：观念创新与实践挑战》，《法学研究》2005年第2期，第3页。

〔84〕 1890年，沃伦与布兰代斯大法官合作发表的美国法律史上最著名的论文之一，也是从权利发展的角度首次提出以“自由生活权”为核心的隐私权概念。See Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

〔85〕 中国消费者协会：《2014年度消费者个人信息网络安全状况报告》（2015年3月13日），第21页。

〔86〕 中国信息通信研究院：《电信和互联网用户个人信息保护年度报告（2014版）》（2015年5月），第38页。

〔87〕 中国互联网络信息中心：《第39次中国互联网络发展状况统计报告》（2017年1月），第86页。

〔88〕 《个人隐私泄漏催生新型犯罪，警方严打买卖公民信息犯罪》，http://news.hexun.com/2013-01-19/150351908.html，2018年1月25日访问。

〔89〕 宪法权利与民事权利的区分，参见于飞：《基本权利与民事权利的区分及宪法对民法的影响》，《法学研究》2008年第5期，第49页。

选择权、变更权、删除权、撤回权等各权项，使信息主体能够真正参与到个人信息保护之中。

大数据时代的个人信息保护是一个崭新的领域，个人信息权属于一项新的权利，权利的性质与边界都还不清晰，不宜简单用传统权利观念剪裁。〔90〕简单照搬传统权利理论，可能会陷入无休止的理论争论之中，耗费大量精力。〔91〕缺乏系统制度支撑的法律规定，口号再响亮，规范意义也会非常模糊，〔92〕在实践中更不可能产生影响。各国实践已经证明，即使立法技术科学，权利体系设计严密，仅仅依靠个人同意权等传统隐私权保护机制，无法应对大数据快速发展背景下的个人信息保护问题，〔93〕告知同意机制完全可能流于形式，信息主体只能选择同意。〔94〕正因为如此，才有欧盟、美国对激励相容机制的共同探索。

这就表明，个人信息保护法在设计治理结构的同时，必须考虑实施环节的激励相容机制实现问题，使实施部门对立法目的和基本制度构造有非常清晰的整体认识，并处理好不同维度之间的关系。个人信息保护法的实施需要循序渐进、突出重点、把握主线，以风险管理与防控为共同切入点，寻求法律实施的最大公约数，梯度递进。首先要通过立法在内的外部机制助推信息控制者组织架构变革，发育有效内生机制，形成内外互动合力，以有效预防绝大部分个人信息安全风险。在此基础上，根据国情、信息控制者接受度和公众偏好等因素，逐步探索提高价值定位，如合规、权利实现等。这种实施策略，既可以形成激励相容合力，调动信息控制者维护信息安全的积极性，降低规制成本，迅速实现基本安全目标，也有利于监管部门集中执法力量，聚焦核心环节，避免执法力量过于分散。比如，对于信息控制者的不合规行为，在既有协商执行的余地又有强制手段的情况下，先协商执行效果可能要比简单强制好，更有利于调动信息控制者持续改进的积极性，而不是一罚了事。再如，个人信息从最内核的隐私信息到通常理解的敏感信息再到最外围的大数据意义上的非敏感个人信息，呈现一个放射状扇形结构。对于不同的个人信息，执行机制就要进行区分，采用不同强度的保护标准，界定信息控制者不同的责任。又如，信息主体权利的实现是一个过程，个人信息保护法中规定的不同权项不可能一步同时到位，执行中必然也

〔90〕 国际上对于消费者权利是否属于人权的讨论，参见 Sinai Deutch, *Are Consumer Rights Human Rights*, 32 Osgoode Hall L. J. 537 (1994)。

〔91〕 对于个人信息权的性质，国内民法学者有很多不同的主张，有宪法权利说、财产性权利说、一般人格权说、具体人格权说、新型的复合性权利说等。这些不同主张基本停留在传统民法学概念体系内，与个人信息保护法制度建构关系不大，与国际上对于个人信息保护的讨论也相去甚远。参见郭明龙：《个人信息权利的侵权法保护》，中国法制出版社 2012 年版，第 44 页；刘德良：《个人信息的财产权保护》，《法学研究》2007 年第 3 期，第 80 页；王利明：《编纂一部网络时代的民法典》，《暨南学报（哲学社会科学版）》2016 年第 7 期，第 8 页；王利明：《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》，《现代法学》2013 年第 4 期，第 62 页；齐爱民：《论个人信息的法律属性与构成要素》，《情报理论与实践》2009 年第 10 期，第 26 页；张素华：《个人信息商业运用的法律保护》，《苏州大学学报》2005 年第 2 期，第 36 页。

〔92〕 比如，民法总则第 111 条规定，“自然人的个人信息受法律保护”。但是，由于第 109 条规定的是一般人格尊严，第 110 条规定的是包括名誉权、荣誉权、隐私权等在内的具体人格权，而第 112 条规定的是人身权。这样的条文结构前后安排，仅就立法技术而言，个人信息是否属于一项权利，该权利与人格权的关系等，均存在很大的不确定性。民法学者对于人格权条款的批评，参见王利明、周友军：《我国〈民法总则〉的成功与不足》，《比较法研究》2017 年第 4 期，第 14 页。

〔93〕 舍恩伯格明确指出，“在大数据时代，不管是告知与许可、模糊化还是匿名化，这三大隐私保护策略都失效了”。参见前引〔17〕，迈尔 - 舍恩伯格等文，第 200 页。

〔94〕 参见范为：《大数据时代个人信息保护的路径重构》，《环球法律评论》2016 年第 5 期，第 94 页。

需要有所区分，根据不同场景设计不同制度。也就是说，个人信息保护法的制定只是完成了一半任务，另一半任务在于实施中的策略选择和具体部署，如何实施法律决定了最初立法目标能否真正实现。

如果打破上述次序，不是先从信息安全风险管理角度切入，由易到难，而是反其道而行之，一下子全部铺开，势必加大内生机制的形成难度，相互牵制、抵消，欲速则不达，事与愿违。中国四十年成功的渐进改革经验对个人信息保护法的实施路径选择有很强的参考意义，需要时时借鉴。实际上，激励相容的制度设计，通过外部威慑促使信息控制者内生机制发挥作用，而不是“一刀切”式的命令控制立法，正是为了在实施环节推动形成多元互动的良好治理格局，以实现立法目标。

Abstract: In the age of big data, data controllers have very strong incentive to use personal information but lack the same incentive to protect them. Therefore, legal rules will not be implemented effectively due to incentive incompatibility, if they only impose various prohibitive or compulsory obligations on the data controller. Though EU and U. S. have adopted different approaches to personal information legislation, among other differences, both of them have been pursuing the establishment of incentive compatible personal information protection regime, especially in recent several years alone with the coming of the age of big data. However, this trend of development has been ignored by most Chinese experts. The current legislation on personal information protection in China have such problems as separation between external legal requirements and data controllers' internal governance structure, disconnection between penal sanctions and other legal remedies, and divorce of behavior obligations from legal consequences. The Personal Information Protection Law should take the fostering of data controllers' internal governance structure as its objective and the establishment of an effective external deterrence mechanism of law enforcement as its safeguard, so as to encourage proactive implementation of responsibility for data security and punish violation of the law. Meanwhile, the Law should recognize the right of the subject of data to control his/her own information in public law, and should not avoid the discourse of fundamental rights. To realize incentive compatibility, China must ensure that the implementation of the Personal Information Protection Law is consistent with the law-making process, proceed from the risk management of information security, and take an incremental, step-by-step approach to the implementation of the law.

Key Words: incentive compatible, Law on the Protection of Personal Data, right of control over person information, information security, the age of big data