交大法学 SJTU Law Review
No. 2 (2020)

我国个人信息保护行政监管的立法选择

邓　辉*

目次

摘要　在大数据时代，个人信息的重要性愈发凸显。作为个人信息保护的第三大支柱，垂直面的监管制度构建与水平面的权利义务设立同样重要。由于顶层设计的缺失和部门分散立法的局限，我国目前的个人信息保护行政监管存在着目标弱化、主体分散、措施乏力和程序模糊等问题，严重阻碍了个人信息保护水平的提高。面对新兴科技的法律挑战与错综复杂的利益平衡需求，未来的个人信息保护立法应当明确行政监管的主要目标，建立统一和独立的监管机构，提升其专业性和行政级别，细化具体的监管措施，并协调不同保护程序之间的关系。

关键词　个人信息保护　行政监管　监管机构　监管目标　监管措施

大数据、区块链等信息技术的不断发展，使得个人信息的重要性前所未有地凸显出来。在现代社会中，随着技术的门槛越来越低，个人信息遭受侵害的情形越来越常见，但是信息主体难以进

* 北京大学法学院博士研究生。本文系北京市法学会重点项目“司法大数据应用的法治保障”（项目编号：BLS[2017]A007）的阶段性研究成果。

行私力救济，只有依靠民法救济、刑事规范和行政监管的合力才能形成对个人信息的全面保护。事实上，个人信息的保护和利用不仅事关公民的基本权利和人格尊严，同时也与经济发展和社会公共利益存在着紧密的联系，还关系着网络主权和国家安全的维护，涉及不同层面的制度安排。除了在水平层面上不断完善（自然人的）个人信息权利和（信息从业者的）个人信息保护义务规定外，立法还应当在纵向层面上建立合理和高效的监管制度，确保关于权利保护、义务遵守和救济提供的规定能够落到实处。〔1〕职是之故，本文拟对我国个人信息保护行政监管的现状进行分析，并从目标、主体、措施和程序等四个方面提出具体的优化路径和改进方向，冀以推动相关立法和实践的发展。

一、我国个人信息保护行政监管现状的梳理分析

（一）存在强烈和现实的监管需求

由于大数据技术的快速发展和广泛运用，信息利用的范围和深度逐渐扩展。被誉为“信息时代原材料”的个人信息，不仅关系着信息主体的人格尊严，还作为基础数据推动着经济社会的持续发展，受到了社会各界的极大重视。近年来，我国关于个人信息保护的立法进程明显加快。2009年，《刑法修正案（七）》增加了“侵犯公民个人信息罪”（《刑法》第253条之一），将“违反国家规定，向他人出售或提供公民个人信息”的行为规定为犯罪行为。2012年，全国人大常委会发布《关于加强网络信息保护的决定》，将“能够识别公民个人身份和涉及公民个人隐私的电子信息”纳入保护范围（第1条）。2013年，工信部和国务院分别发布了《电信和互联网用户个人信息保护规定》和《征信业管理条例》来规范电信业务、互联网信息服务以及征信业务等领域中的个人信息利用行为。2016年，《网络安全法》首次在立法层面通过“定义＋不完全列举”的方式来界定“个人信息”（第76条第5项）。2017年以来，《测绘法》《公共图书馆法》和《电子商务法》等多项立法也都对各自领域内的个人信息保护进行了规定。

随着立法进程的进一步加快，对个人信息的多重保护机制逐步建立。在个人信息遭受侵害时，受害人可以选择私力救济和司法救济等不同的权利救济方式。同时，在社会规制层面，信息产业或互联网行业协会也可以建立以行业标准为代表的自律机制，来防止或纠正个人信息侵害行为。〔2〕然而，上述的应对措施都存在力有未逮之处：首先，私力救济不具备现实基础。在实践中，通过网络手段侵害个人信息的行为具备技术性、虚拟性和迅速性等特性，信息主体（信息权利人）难以进行预防。〔3〕不仅如此，行为人有时还通过技术手段隐蔽其真实身份，信息主体根本无法查实具体的责任人，更遑论进行自力救济。其次，司法救济存在效率上的缺陷。作为“社会公平正义的最后一道防线”，司法救济能够为当事人提供最全面的权利保护和程序保障。但是，司法救济通常只针对已经发生的侵害行为，无法对潜在的威胁进行预先防范。受害人想要通过诉讼手段

---

〔1〕 有学者认为，欧洲个人数据保护赖以建立的三大支柱包括数据主体的权利、数据控制者与处理者的义务和国家主管机关的监管。See Andra Giurgiu & Tine A. Larsen, *Roles and Powers of National Data Protection Authorities — Moving from Directive 95/46/EC to the GDPR: Stronger and More “European” DPAs as Guardians of Consistency?*, 2 European Data Protection Law Review 342－352 (2016).

〔2〕 参见刘晓春：《大数据时代个人信息保护的行业标准主导模式》，载《财经法学》2017年第2期，第17—21页。

〔3〕 参见刁胜先：《个人信息网络侵权责任形式的分类与构成要件》，载《重庆邮电大学学报（社会科学版）》2014年第2期，第31页。

获得司法救济，往往因为繁琐的程序而需要付出大量的时间和精力，不能对恶意侵害事件进行快速和有效的反应。〔4〕再次，我国相关的行业自律机制尚未形成。目前，我国信息产业取得了飞速的发展，但关于个人信息保护的自律性行业规定仍旧付诸阙如。在用户个人信息的商业化利用过程中，包括“徐玉玉事件”在内的个人信息泄露事件层出不穷，不断引发要求加强相关企业个人信息保护责任的呼吁。〔5〕究其原因，互联网企业或行业具备天然的逐利性，使得为市场决策服务的信息利用思维占据了主导地位。简单地说，市场主体对个人信息的态度主要表现为“重商业利用、轻法律保护”，缺乏足够的动力来进行自我管理和制定相应的保护政策。〔6〕因此，在未来一段时期内，只有进一步加强外部监督和执法威慑，才能够促使信息从业者认识到个人信息保护的重要性，逐步实现行业自律和自我管理。〔7〕

相较于以上三种保护手段，行政监管不仅贯穿事前预防、事中监督和事后处理等个人信息保护的全过程，也可以综合运用包括风险管理、调查和处罚等多种手段，还在制止侵权行为方面具备快速和便捷的特点，能够充分应对现实中的各种挑战，从而为个人信息提供多角度和全方位的保障。再者，在国家治理体系和治理能力不断现代化的背景下，政府职能基本实现了从“管理型”到“服务型”的转变，但是，公权力机关仍可以对个人信息保护等事关公共福祉的重大领域进行监管。此外，由于公共管理职能的明确要求和有力的制度保障，行政监管既能够为个人信息提供更周延的保护，又可以妥善处理公民权利保护、网络安全维护和经济社会发展之间的关系。由此可见，我国建立个人信息保护监管制度，既具备相当明显的比较优势，同时也契合现实社会的发展需要。

（二）相对弱化和附属的监管目标

2016年通过的《网络安全法》不仅系统地定义了个人信息的概念和范围，还明确了责任主体的行为义务，应当属于目前最重要的个人信息保护法规。但是，该法的立法目的包括“保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展”等多重目标（《网络安全法》第1条）。〔8〕如此看来，“个人信息保护”仅是“保护公民、法人和其他组织的合法权益”之一环，在网络和信息技术迅猛发展的背景下，反倒处于立法目的体系中与其重要性极不相称的弱小和附属地位。另一方面，由于立法目的上的限制，相应的监管职权配置也未得到应有的重视。比如，国家互联网信息办公室（以下简称“网信办”）的设立是为了“维护互联网安全”和“加强网络信息保护”，〔9〕其工作重心仍在于“网络安全工作”，而“个人信息保护”最多只能被解释为网信办的“相关监督管理职责”（《网络安全法》第8条第1款）。有学者敏锐地指出：“网络行政管理机关事务繁多，需要负责网络安全的各个方面，在资源有限的

〔4〕 参见张平：《大数据时代个人信息保护的立法选择》，载《北京大学学报（哲学社会科学版）》2017年第3期，第150页。

〔5〕 参见王叶刚：《保护个人信息，相关企业责无旁贷》，载《光明日报》2016年11月7日，第10版。

〔6〕 参见周汉华：《探索激励兼容的个人数据治理之道——中国个人信息保护法的立法方向》，载《法学研究》2018年第2期，第6页。

〔7〕 2019年，一款名为“ZAO”的换脸软件强制要求用户授予“全球范围内完全免费、不可撤销、永久、可转授权和可再许可的权利”。有学者建议就此建立强有力的专门监管机构及设立巨额罚款。参见何渊：《无牙的法律——ZAO为何敢如此肆无忌惮地ZUO?！出路：打造中国版的FTC及设立巨额罚款》，载微信公众号“数据法盟”，https://mp.weixin.qq.com/s/_YGOmOubdznv4LJcagmBNw。

〔8〕 参见杨合庆主编：《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37—40页。

〔9〕 参见《全国人民代表大会常务委员会关于维护互联网安全的决定》和《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》。

情况下，行政机关往往侧重于国家和社会重大安全网络事件的监管，而相对次要的个人信息保护则容易疏于监管。”〔10〕

在消费者个人信息保护领域，《消费者权益保护法》需要兼顾“保护消费者的合法权益”“维护社会经济秩序”和“促进社会主义市场经济健康发展”等不同的立法目的（《消费者权益保护法》第1条）。在这些立法目的中，“保护消费者的合法权益”属于《消费者权益保护法》的“基础和核心”。〔11〕但是，“消费者个人信息受保护的权利”在消费者权利体系中仅占半句（《消费者权益保护法》第14条后半句），实在难以彰显个人信息保护的重要性。

由此可见，在我国个人信息保护分散立法的背景下，单行法或部门法限于其本身的立法目的，通常将维护公共利益、促进经济发展和维护社会秩序等立法目标置于相对优先的地位，导致“个人信息保护”在部门监管目标中呈现出附带性或从属性的特征，不利于个人信息保护的监管和信息主体合法权益的保障。

（三）缺乏统一和独立的监管机构

目前，在我国行业分散立法的背景下，个人信息保护监管呈现出明显的部门区隔特征：在一般消费领域，工商行政部门和其他有关部门负责保护消费者的个人信息权利（《消费者权益保护法》第32条）；在电信和互联网领域，主要由国家网信部门、电信主管部门、公安部门和其他有关机关对个人信息保护工作进行监管（《电信和互联网用户个人信息保护规定》第17条、《网络安全法》第8条）；在征信和邮政快递领域，个人信息保护监管分别由国务院征信业监督管理部门（中国人民银行）和国家邮政管理机构（国家邮政局）负责。（参见下表1）

表1　我国目前个人信息保护的监管概况

领域	监管对象	法律规范	监管机构	职责分工	监管措施
消费	经营者	《消费者权益保护法》	工商行政部门和其他有关行政部门	依照法律、法规的规定，在各自的职责范围内，采取措施，保护消费者的合法权益。	警告、没收违法所得、罚款、责令停业整顿、吊销营业执照。
电信	电信业经营者	《电信和互联网用户个人信息保护规定》	电信管理机构	对电信业务经营者、互联网信息服务提供者保护用户个人信息情况实施监督检查。	要求提供相关材料，进入生产经营场所调查。
互联网/网络	互联网服务提供者				限期改正、警告、罚款。
	网络运营者、网络产品或者服务的提供者	《网络安全法》	国家网信部门	统筹协调网络安全工作和相关监督管理工作。	警告、没收违法所得、罚款、责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。
			电信主管部门、公安部门和其他有关机关	依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。	

〔10〕 蒋都都、杨解君：《大数据时代的信息公益诉讼探讨——以公众的个人信息保护为聚焦》，载《广西社会科学》2019年第5期，第110页。

〔11〕 参见李适时主编：《中华人民共和国消费者权益保护法释义》（最新修正版），法律出版社2013年版，第3页。

续表

领域	监管对象	法律规范	监管机构	职责分工	监管措施
征信	征信业和金融信用信息基础数据库运行机构	《征信业管理条例》	国务院征信业监督管理部门及其派出机构	依法对征信业进行监督管理。	1.实施包括现场检查、询问、查阅、复制和封存资料文件以及检查相关信息系统在内的监督管理措施。2.责令改正、没收违法所得、进行罚款。
	商业银行	《个人信用信息基础数据库管理暂行办法》	中国人民银行征信服务中心	承担个人信用数据库的日常运行和管理，建立完善的规章制度和采取先进的技术手段确保个人信用信息安全。	责令改正、处以罚款。
邮政快递	经营快递业务的企业	《快递暂行条例》	国务院邮政管理部门	会同国务院有关部门制定电子数据管理制度等具体办法。	责令改正、没收违法所得、处以罚款、责令停业整顿、吊销快递业务经营许可证。
	邮政企业 快递企业	《寄递服务用户个人信息安全管理规定》	邮政管理机构	负责全国、本行政区域或本辖区内的邮政行业寄递用户信息安全监督管理工作。	1.加强宣传、强化信息安全管理意识、提高用户认识。2.进行调查处理、依法进行处罚。

由于立法上缺乏对监管机构的统一规定，我国个人信息保护的实践已经受到严重影响。例如，部分领域的立法完全没有规定监管主体。《商业银行法》《执业医师法》和《旅游法》确立了金融、医疗和旅游领域中个人信息受保护的规定，但是，由于缺乏对监管主体、监管措施和法律责任的规定，基本等同于没有相应的监管机构来履行监管职责。又如，即便根据法律规定，也难以确定具体的监管机构。在消费者和网络个人信息保护的领域，对于所谓“有关行政部门”(《消费者权益保护法》第32条)以及“有关机关”(《网络安全法》第8条第1款)究竟是指哪一具体的行政部门或机关，立法并没有进行明确的说明，可能导致负有监管义务的机关相互推诿、逃避职责。再如，部分行业或领域的多头监管，容易引发管辖中的混乱。“工商行政管理部门”(《消费者权益保护法》第32条)以及“电信主管部门和公安部门”(《网络安全法》第8条第1款)仅对涉及“消费者权益”与“网络信息安全”的个人信息侵害行为进行监管。那么，在侵害经营者的个人信息但尚未危害网络安全或构成犯罪时，即出现了监管的“空白区域”；在行为人利用电信或网络盗卖消费者个人信息时，又存在“重复监管”的现象。

(四)缺少细致和有效的监管措施

我国个人信息保护法规通常赋予监管机构进行调查和处罚的权力(参见表1)。但是，总的来说，这些措施还存在着介入阶段滞后、保护手段匮乏的问题：

1.事先防范缺乏有效机制，法律约束动力不足。基于对平衡信息产业发展和个人信息权利保护之间关系的考量，我国不应进行过多的事前限制。在法律没有明确禁止的前提下，只要取得信息主体的同意，信息处理者就有权对个人敏感信息和一般信息进行处理，无须事先由监管机构进行审查或取得监管机构的许可。然而，这不等于立法应当放弃个人信息保护的事先预防。目前，

我国的信息安全风险管理体系已经基本建成，相关的国家标准和地方政府规章涵盖了信息安全风险评估、管理和处理等主要领域。但是，传统意义上的信息安全主要规制计算机系统的运行安全，基本没有将个人信息保护纳入考量。〔12〕这意味着，信息安全管理制度与个人信息保护仍然处于脱节的状态，无法预防或减轻因信息泄露带来的损害。

2. 事中监督大量使用“行政约谈”，非正式手段措施乏力。在信息收集和处理行为涉嫌侵害公民的个人信息时，监管机构的通常做法是通过约谈来约束相关企业的行为。例如，在“2017 年支付宝年度账单”事件中，负有监督检查职责的网信办以及工信部信息通信管理局先后在 2018 年 1 月 6 日和 11 日约谈当事企业的负责人，要求相关企业进行整改。〔13〕然而，这种被广泛运用的“行政约谈”手段，其主要功能在于警示、告诫或指导，缺乏相应的强制力，〔14〕不仅在行为性质上尚待进一步的理论澄清和检验，而且在对监管对象的程序保障以及约谈的法律效力等方面也面临着诸多质疑。〔15〕从我国实践的情况来看，往往是侵犯个人信息的行为已经发生，监管机构才采取本应在事前进行的约谈措施，无法真正起到对侵害行为的预防和制止作用。

3. 事后处罚的力度较轻，难以实现有效的威慑。针对支付宝（中国）网络技术有限公司在个人信息保护方面存在的违法行为，中国人民银行杭州中心支行依据《消费者权益保护法》对其处以警告和 5 万元罚款。〔16〕但是，通常来说，行政监管采取营业地管辖原则，这样的规定已经足以避免不同的监管机构对同一违法行为进行多次处罚。为了实现对个人信息侵害行为的威慑，立法在“没收违法所得”外还应当确定一个较高的处罚数额（固定数额）或将获利因素（比如年营业额）纳入考量。〔17〕准此而言，在实践中，由于缺乏明确和具体的客观标准和考量因素，我国对个人信息违法行为的处罚力度偏低，难以实现威慑和遏制的目的。

二、我国个人信息保护行政监管目标的合理设置

（一）以“强化私权保护”为主要目标

《民法总则》第 111 条立法采用的措辞是“个人信息”并非“个人信息权”。按照严格的文义解释，个人信息属于受法律保护的“法益”（合法利益），仅表明对个人信息进行保护的基本立场。〔18〕但是，从体系解释和目的解释来看，《民法总则》第 111 条本身存在着极大的权利解释空间，应当被解释为个人信息的确权规范。〔19〕更关键的是，在个人信息日益成为一种重要社会资源的背景下，

---

〔12〕 参见前注〔6〕，周汉华文，第 13—14 页。

〔13〕 参见《国家互联网信息办公室网络安全协调局约谈“支付宝年度账单事件”当事企业负责人》，载国家互联网信息办公室网站，http://www.cac.gov.cn/2018-01/10/c_1122234687.htm；《信息通信管理局就加强用户个人信息保护约谈相关企业》，载工业和信息化部网站，http://www.miit.gov.cn/n1146290/n1146402/n1146440/c6010817/content.html。

〔14〕 参见徐永涛、林树金：《我国行政约谈的理论基础及法治化》，载《东岳论坛》2014 年第 12 期，第 168 页。

〔15〕 参见郑毅：《现代行政法视野下的约谈》，载《行政法学研究》2012 年第 4 期，第 57—59 页。

〔16〕 由于支付宝在客户权益和产品宣传方面的违法行为，还被分别处以 3 万元和 10 万元的罚款。参见中国人民银行杭州中心支行杭银处罚字〔2018〕23 号行政处罚决定书。

〔17〕 例如，《欧盟一般数据保护条例》（GDPR）第 83 条规定，在被监管对象严重违反数据保护规定时，监管机构可以处以 2 000 万欧元或其财政年度全球收入 4%（取其高者）的罚款。

〔18〕 参见叶金强：《〈民法总则〉“民事权利章”的得与失》，载《中外法学》2017 年第 3 期，第 651 页。

〔19〕 参见王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019 年第 6 期，第 140—141 页。

只有以表彰私权属性为基础，才能够在现实和未来的层面上对个人信息进行有效的规制和保护。〔20〕换言之，个人信息并非仅为“法益”，而是属于私法上的重要“权利”，从而能够享有更高层次的法律保护。〔21〕

近代以来，正当的政治和法律秩序必须以个体权利（私权）为核心，逐渐形成了作为私法基础的权利本位观念。〔22〕即使在公法领域，立法者也必须正视相关制度对个人权利的影响。〔23〕主流观点认为，“个人信息权”是一种具体人格权，〔24〕同时也属于基本权利，因而具备客观法的性质：一方面，所有组织和个人必须尊重这种民事权利，不得进行侵害；另一方面，包括监管机构在内的公权力机关也负有义务进行更周延和完整的权利保护，采取积极措施来创造和执行制度性保障，进而营造个人信息权受保护的客观价值秩序。〔25〕在这个意义上来说，“权利保护”应当成为个人信息保护监管的主要目标和监管机构的主要职责。

（二）扮演“利益冲突协调者”的角色

尽管个人信息保护的最有利方式是进行完备周全的综合立法，但这种方式可能无法兼顾信息产业发展的需求，并阻碍信息的自由流通。〔26〕在进行个人信息保护法律制度构建时，需要在信息主体（个人基本权利）、信息行业（经营活动）和国家管理（公共利益）三方之间进行更多的利益平衡。〔27〕进一步而言，在个人信息保护中发生利益冲突时，由于信息主体（个人）和信息从业者（经营者）存在实际能力和利益取向上的局限性，个人信息保护监管机构作为法律实施状况的监督者和公共利益的代表，理应承担起协调利益冲突的责任。

在立法没有明文规定的前提下，如果个人信息权利与下列的公共利益或他人重大利益发生冲突，监管机构应当运用比例原则等利益衡量方法来进行妥当的处理：（1）国家安全和国防安全，针对个人信息（数据）跨境流通应当采取更加严格的监管措施；（2）公共利益，比如公共安全、公共卫生以及基于公共利益进行的统计、编写历史或学术研究；（3）司法活动，包括侦查、起诉、审判和判决执行等活动；（4）公民的基本权利和自由，比如隐私权、肖像权和言论自由；（5）信息从业者的重大合法权益，比如商业秘密、信息产业发展。此外，在信息主体存在恶意或滥用权利时，其权利行使也应当受到限制。

（三）以“信息社会治理”为基本理念

进入信息化时代以来，信息主体、信息从业者（控制者和处理者）、社会公众等多元主体的参与和互动成为有目共睹的事实，单纯依靠自上而下的命令已无法确保法律规则的严格遵守。〔28〕因此，面对不同主体的利益诉求，构建有序的参与机制才是治本之道。有学者指出，社会治理作为管理的升级版，承载着更多的职能，其主要特点就是允许适当的自治空间与社会的多元参与，从而逐

〔20〕 参见王利明：《论个人信息权在人格权法中的地位》，载《苏州大学学报》2012年第6期，第75页。

〔21〕 参见杨立新：《个人信息：法益抑或民事权利》，载《法学论坛》2018年第1期，第40页。

〔22〕 参见周濂：《后形而上学视阈下的西方权利理论》，载《中国社会科学》2012年第6期，第50—51页。

〔23〕 参见刘权、应亮亮：《比例原则适用的跨学科审视与反思》，载《财经法学》2017年第5期，第42—43页。

〔24〕 参见王利明：《论个人信息权的法律保护》，载《现代法学》2013年第4期，第70页。

〔25〕 参见张翔：《基本权利的双重性质》，载《法学研究》2005年第3期，第28页。

〔26〕 参见蒋坡主编：《个人数据信息的法律保护》，中国政法大学出版社2008年版，第112页。

〔27〕 参见张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，载《中国法学》2015年第3期，第52页。

〔28〕 由于现代社会系统结构的复杂性和不确定性，传统意义上的科层式管制（管理）体制难以解决信息时代的难题。参见范如国：《复杂网络结构范型下的社会治理协同创新》，载《中国社会科学》2014年第4期，第99页。

渐形成个人信息保护与利用的制度性激励，进而实现综合治理的新格局。〔29〕

维护网络安全和推进信息化等公共利益的实现，既需要监管机构采取行政管理措施进行有效的监督，也需要信息控制者和处理者的共同协力。尤其是，针对个人信息的合规化处理，更加依赖不同主体之间的合作。比如，作为技术性实际操作规则的《信息安全技术 个人信息安全规范》(GB/T 35273—2017)中的若干规定就直接体现了个人权利保护指引、企业合规参考和国家推荐标准三种意义。〔30〕可见，个人信息保护监管应当置身于“信息社会治理”的大背景下，关注和重视包括市场与信用在内的其他社会力量，〔31〕为行业自律机制和舆论监督发挥作用预留下足够的空间，积极引导多种社会因素的有序参与并进行有效的监督。

三、我国个人信息保护行政监管主体的立法设想

（一）域外主要国家和地区的立法与实践

早在1995年，《欧盟数据保护指令》(Directive 95/46/EC)即要求各成员国成立监管机构(supervisory authorities)来确保前述指令的适用。为了正确地履行保护数据权利和促进数据流通的职能，这些公共机构应当独立存在，并有权实施包括进行调查、干预以及介入诉讼等方式在内的行政监管措施。不仅如此，2018年5月25日起实施的《欧盟一般数据保护条例》(General Data Protection Regulation/GDPR)除了实现个人数据保护统一立法和确立广泛的数据权利外，其所推行的对个人信息保护的强力监管也颇为引人瞩目，尤其是GDPR不仅建立了全覆盖、多层次的监管体系，而且大大细化了对监管机构的组织独立性、目标定位和职责范围等方面的具体要求。〔32〕

在欧盟范围来看，尽管在名称和监管模式上存在些许差异，大多数成员国都已经建立了本国的个人信息保护监管机构。〔33〕英国和德国的情况也大致相同：即便英国已经启动“脱欧”程序，但是个人信息保护仍被视为重要的议题。根据2017年《英国数据保护法案》，作为监管机构的“信息专员办公室”(Information Commissioner's Office)将继续保持独立性，并获得更大权力来处理相关投诉、进行调查、罚款和刑事制裁。〔34〕在德国，2015年修订的《联邦数据保护法》要求国家数据保护监督机关负责监督和确保个人数据保护条款的执行，有权在监管目的范围内对数据进行加工、使用或传输。〔35〕

在分散式行业立法的框架下，美国虽然没有统一的监管机构，但更加重视个人信息保护的执法实践，采取了灵活多样的执法手段。迄今为止，美国尚未形成综合性的个人信息保护法典或法

---

〔29〕 参见前注〔6〕，周汉华文，第4—5页。

〔30〕 参见吴沈括：《个人信息保护的规范趋势：走向客观综合主义保护》，载《中国信息安全》2018年第3期，第72页。

〔31〕 参见余佳、刘逸帆、葛云：《加强个人信息保护、促进社会和谐进步——访中国电子商务协会政策法律委员会副主任阿拉木斯》，载《社会治理》2017年第5期，第41页。

〔32〕 Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer International Publishing AG, 2017, p.189-190.

〔33〕 参见高志明：《个人信息保护中的自律与监督》，载《青岛科技大学学报(社会科学版)》2016年第3期，第88页。

〔34〕 参见英国数字、文化、媒体和体育部(DCMS)：《英国新数据保护法案：改革计划》，邓辉译，载《中国应用法学》2017年第6期，第174页。

〔35〕 参见任文倩：《德国〈联邦数据保护法〉介绍》，载《网络法律评论》2016年第1期，第69页。

律，相关的联邦立法仅规定了各领域或行业的主管机关，由其负责监督和管理本行业内个人信息（隐私）保护的实施情况。比如，美国联邦贸易委员会（FTC）承担了大部分消费者个人信息保护的监管职能，消费者金融保护局（CFFB）负责与征信和金融有关的个人信息监管，而关于通讯和医疗的个人信息保护则分别由联邦通信委员会（FCC）与卫生和公共服务部（HHS）进行监管。其中，FTC不仅有权要求进行专项整改、命令删除非法获得的消费者信息、没收非法所得以及进行其他行政处罚，同时也致力于通过制定规则、发布指南与举办培训班等方式来实现对消费者个人信息的严格保护。截至2018年底，FTC已经处理了上千起关于个人隐私和数据安全的案子，从而保护了上亿消费者。〔36〕有学者指出，FTC的执法实践不仅直接对消费者的个人信息提供保护，还间接地塑造了美国的隐私和个人信息法律制度。〔37〕

在东亚地区，根据《韩国个人信息保护法》（2011年）和《日本个人信息保护法》（2015年修订）的规定，作为个人信息保护监管的专责机关，新设立的“个人信息保护委员会”直属于总统或内阁总理大臣，负责统筹个人信息保护并享有相应的行政职权。〔38〕与此同时，在我国香港地区，“个人资料私隐专员（公署）”负责《个人资料（私隐）条例》的实施和个人资料的保障，并密切关注国际发展趋势与香港地区的社会期望，对个人资料的保护需求做出及时和有效的回应。〔39〕在我国澳门地区，按《个人资料保护法》第28条和《民法典》第79条的规定，监察个人资料的收集、储存与使用的主管机构为“公共当局”。但是，这样的规定过于模糊，特区政府在2007年设立了“个人资料保护办公室”作为专责的监管机构。我国台湾地区“个人资料保护法”第22条规定，“‘中央’目的事业主管机关”和“‘直辖市’、县（市）政府”是行政监管机构，但是，当局迟迟未设立专责的监管机构，引发了人们对法律实施效果的质疑。〔40〕

（二）既有的立法建议及其局限

对于个人信息保护的立法，我国学者积极开展理论研究，并提出了数个具有重大立法参考价值的草案建议稿。其中，由齐爱民教授提出的《个人信息保护法示范法草案学者建议稿》区分了国家机关与非国家机关，涵盖了个人信息的收集、处理和利用以及相应的损害赔偿，但是，该建议稿缺乏对个人信息保护监管的相关规定。〔41〕周汉华教授主持的专家建议稿及说明指出，在缺乏个人信息保护法专门执行机构的背景下，建议成立“专门的政府信息资源主管部门”对个人信息处理进行政府管理，负责相应的登记、许可、审查和决定等事项（第35—41条）。在有条件的情况下，也

〔36〕 Federal Trade Commission, *Privacy & Data Security Update: 2018*, https://www.ftc.gov/reports/privacy-data-security-update-2018.

〔37〕 Daniel J. Solove & Woodrow Hartzog, *The FTC and The New Common Law of Privacy*, 114 Columbia Law Review 583-584 (2014).

〔38〕 参见郭戎晋：《韩国个人资料保护法制之比较研究》，载《科技法律透析》2014年第2期，第33—34页；范姜真媺：《日本个人编号法对我国之借镜——以个人资料保护监督机制为主》，载《东吴法律学报》2014年第2期，第22—23页。

〔39〕 Stephen Kai-yi Wong & Guobin Zhu, *Personal Data (Privacy) Law in Hong Kong*, The City University of Hong Kong Press, 2016, p.3-5.

〔40〕 参见罗承宗：《无专责机关的二代个资法：一个资料探勘的尝试》，载《新社会政策》总第10期（2010年6月），第30、32页；李飞：《台湾“个人资料保护法”的变迁、问题及其启示意义》，载《厦门大学法律评论》（第20辑），厦门大学出版社2012年版，第286—288页。

〔41〕 参见齐爱民：《中华人民共和国个人信息保护法示范法草案学者建议稿》，载《河北法学》2005年第6期，第2—5页。

可以吸收政府之外的专家，共同组建“独立的信息委员会”。〔42〕在张新宝教授主持起草的《个人信息保护法》（专家建议稿）中，“监督管理”（第六章）制度设计的基本思路是“在坚持网信部门核心地位的同时，充分发挥新闻监督、社会监督和公共参与的作用”，主张“网信办牵头协调，共同参与”。〔43〕

值得注意的是，《网络安全法》出台以来，“网信办”在个人信息保护领域中发挥着愈加重要的作用。但是，“网信办”与“中央网络安全和信息化领导小组办公室”是“两块牌子、一套机构”，后者在组织建制上仅是议事协调机构，属于一种“阶段性工作机制”，不是严格意义上的实体性组织，其专业性和独立性难以获得保障。在此背景下，即便立法赋予了“网信办”进行统筹协调的职权，它也无法摆脱临时组织的性质和多头监管带来的弊端。这充分表明，分散式的监管主体缺乏统一性和独立性，无法有效地统领个人信息保护监管的大局。

（三）建立统一和独立的监管主体

如前所述，我国目前个人信息保护仍处于分散立法阶段，由多个部门进行分别监管，相应的监管主体设置和职权配置也牵涉网信部门、工信部门、公安机关、邮政管理部门以及人民银行等多个主体。但是，相互独立的行业监管无法实现统一健全的顶层设计，个人信息保护的监管体制难以实现突破，而不同监管机关之间的冲突协调又困难重重。〔44〕因此，在未来的民法典分则或个人信息保护单行法中，立法应当新设立以“个人信息保护”为主要目标的专责监管机构，采取统一而非分散的监管模式，打破不同行业之间的藩篱，实现更高程度的统筹、协调和指导，促进个人信息保护监管的统一领导与国际合作。

世界上主要国家和地区的立法和实践表明，只有坚持个人信息保护监管机构的独立性和全局视野，才能有效地防止和排除其他组织和个人的干预，进而履行法定的监管职能。这种独立性要求具体表现为“人、财、物”等方面的相应保障：在组织结构上，监管机构应当是政府的直接组成部门，而不从属于其他非以个人信息保护为主要职能的政府机关；在人员组成上，监管机构的工作人员属于公务员序列，不得从事与其职业不兼容的活动，尤其是影响履行监管职能的营利性活动；在财政预算上，立法应当保障监管机构享有独立的财政预算，并将其作为国家财政预算的组成部分；在物质条件上，为了履行监督和管理职责，尤其是调查个人信息保护情况，必须保证监管机构具备相应的办公设备及基础设施。

（四）提升专业性和行政级别

在大数据时代，现代社会的信息化程度不断提高，侵害个人信息的行为也呈现出较强的技术性特点，给监管工作带来了巨大的挑战。所以，行政监管机构的设置不仅应当符合专业性的要求，同时也需要其工作人员通过不断学习来提高自身的业务能力，以适应日新月异的个人信息保护环境。除此之外，监管机构还可以效仿“行政复议委员会”的做法，邀请具备信息技术、审计、管理和法律等方面专业知识的人士（专家）协助制定监管法规、处理投诉和进行政策宣传。

对于个人信息保护监管机构的组织形式来说，“委员会”通常属于成建制的固定机构，是为完

---

〔42〕 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，第 83—84 页。

〔43〕 参见《更严厉的数据保护法来了，〈个人信息保护法〉（专家建议稿）即将发布》，载搜狐新闻网，http://www.sohu.com/a/226016805_453795。

〔44〕 参见窦海阳：《民法典有关个人信息立法的立法建议》，载陈甦主编：《中国社会科学院民法典分则草案建议稿》，法律出版社 2019 年版，第 493 页。

成一定的任务而设立的专门组织，其职能更加全面、机构更加规范、运行更加稳定、组织更加健全。在不断推进国家治理体系和治理能力现代化的背景下，机构改革的长远方向是要逐步实现从“领导小组”到“委员会”的转变。〔45〕因此，在未来的立法中，我国应当重视个人信息保护监管的顶层设计和总体布局，尽快设立直属于中央人民政府（国务院）的“个人信息保护委员会”。

四、我国个人信息保护行政监管的措施细化和程序衔接

（一）行政监管措施的细化方案

在数字经济时代，企业经营者受到经济利益的强大驱动，信息行业规范的自觉发展又不充分，往往无视法律法规而实施侵害个人信息的行为。〔46〕退一步来说，即使依靠行业自律机制来实现个人信息的保护，同样也离不开行政监管的外部压力。在这个意义上，行政监管需要而且应当具备行之有效的具体措施，全方位地覆盖个人信息保护的不同阶段。

首先，严格事前防范，建立信息处理风险评估制度。为了在个人权利、公共利益和信息产业发展之间实现适当的平衡，立法应当加强对信息处理活动的“事先评估”。通过对相关的信息处理行为进行事先的风险评估，“个人信息影响风险评估制度”能够明确这些活动对个人信息安全的影响，进而对高风险的信息处理活动采取严格的行政监管。〔47〕同时，由于个人信息的泄露可能导致对信息主体、利害关系人以及社会公共利益造成重大影响，立法还应当在事先确立统一的“信息泄露通知和报告制度”，要求信息控制者和处理者在发生或者可能发生信息泄露、毁损、丢失的情况时立即采取补救措施，及时报告监管机构（有关主管部门）并通知信息主体以及可能受到影响的利害关系人，避免损害的进一步扩大。

其次，加强事中监督，完善监督检查措施。其一，进一步细化监督检查的形式。对于个人信息保护的实施情况，监管机构可以进行监督抽查、专项检查和其他监督检查。对于信息处理系统，监管机构有权选择“现场检查”或“远程检测”等具体方式，以及采取询问、查阅、复制或封存相关资料等措施。其二，设置重点检查对象和内容。对于两年内曾发生过个人信息泄露或网络安全事件的信息控制者和处理者等对象，以及监管对象是否进行登记备案和风险评估、建立信息泄露通知和相关防范制度等内容，监管机构可以进行重点检查。其三，还应当规定监督检查的法律程序。比如，在进行现场检查时，检查人员不得少于两人，并应当出示执法证件和《执法检查通知书》。〔48〕

再次，健全调查处理制度，明确行政处罚的种类。监管机构可以主动进行调查，也可以基于信息主体的申诉进行调查。在后一情形中，监管机构应当在一定期限内进行调查，并将处理结果及时通知申诉人。如果信息控制者和处理者违反有关个人信息保护的法律、行政法规和部门规章，监管机构可以根据情节轻重，采取包括警告、限期改正、没收违法所得、处以罚款、责令停业整顿、吊销营业执照或相关业务经营许可证在内的一种或数种行政处罚措施。

复次，进行事后的追踪观察，重视政策制定和法规宣传。个人信息保护的监管是一个长期和

〔45〕 根据《中共中央深化党和国家机构改革方案》的要求，“中央网络安全和信息化领导小组”将改为“中央网络安全和信息化委员会”。参见《从“领导小组”到“委员会”：全面深化改革进入新阶段》，载中国共产党新闻网，http://theory.people.com.cn/n1/2018/0329/c40531-29895329.html。

〔46〕 参见杜鑫：《每个诈骗案背后都有一本个人信息泄露的“糊涂账”》，载《工人日报》2017年3月5日，第4版。

〔47〕 参见《信息安全技术 个人信息安全影响评估指南（征求意见稿）》。

〔48〕 关于监督检查较为系统和详尽的规定，可参见《公安机关互联网安全监督检查规定》。

持续的过程，应当避免治标不治本的“运动式治理”。对于发生个人信息泄露或网络安全事件的企业，立法可以借鉴《侵权责任法》第64条规定的“产品跟踪观察义务”，要求监管机构进行后续的追踪观察或重点检查，跟进其个人信息保护的整改情况。此外，监管机构还应当制定相应的个人信息保护政策，定期举行法规和政策的培训，培育重视个人信息保护的价值观并引导相关的信息处理行为，以强化多元参与凝聚社会共识，进而促进整个社会的观念更新。

最后，强化信息跨境流通的监管，积极参与国际合作。随着国际经济贸易联系的不断深入，跨国经营中的个人信息储存和出境问题逐渐凸显：一方面，为了保障个人信息安全，维护网络空间主权和国家安全、社会公共利益，世界上主要国家和地区已经要求个人信息储存本地化以及在出境时进行安全评估。〔49〕根据《网络安全法》第37条和相关规定的要求，个人信息境内存储和出境安全评估等法律规则的有效落实，无法离开监管机构的认真履职和积极作为。〔50〕另一方面，为避免形成个人信息保护的“洼地”现象，我国监管机构还应当主动参与双边性、区域性和全球性的国际合作，与其他国家和地区的监管机关展开交流和互动，对内不断提升我国的个人信息保护水平，对外维护我国公民和企业的合法权益、国家利益和社会公共利益，共同应对信息跨境流通监管的世界挑战。

（二）与其他保护程序之间的协调

在现代社会中，个人信息侵害行为日益呈现出技术性、突发性和隐蔽性的特点，私力救济的适用空间被不断压缩，以行政监管与司法救济为代表的公力救济手段则获得了较大的发展。因此，在个人信息保护立法中，应当着力处理好不同保护程序之间的关系，共同协力形成对个人信息的全面保护。

首先，协调个人信息保护行政申诉和民事诉讼之间的关系。作为个人信息保护监管的组成部分，行政申诉制度旨在处理信息主体的投诉，即在个人信息遭到不具有公共管理职能的组织或个人侵害时，权利人（信息主体）可以请求监管机构依据行政程序解决相关争议。〔51〕但是，本制度的设立初衷在于扩大而非限制对个人信息的保护，故不应成为信息主体获得司法救济的前置程序。易言之，在个人信息侵害来自非公务机关时，权利人既可以提出申诉，也可以直接提起诉讼。此外，在大规模的个人信息侵害事件中，受害人为数众多，立法应当规定由其中一人或数人代表全体进行集体诉讼。在必要时，还可以授权消费者保护协会、行政监管机构、人民检察院或合乎法律规定的其他非营利组织提起公益诉讼。

其次，协调行政监管和行政诉讼之间的关系。因履行公共管理职能的需要，公权力机关可以在法律授权的范围内对个人信息进行处理。在这一过程中，行政机关与信息主体之间形成的是行政法律关系。如果公权力机关侵害了公民的个人信息权利，应当先经过行政机关内部的审查和处理，需要遵循“先复议、后诉讼”的原则。另一方面，由于监管机构在本质上也是公权力机关，如果信息主体的申诉在法定期间内没有获得处理或被监管对象不服监管机构的监管措施和处理结果，那么，信息主体或被监管对象也可以监管机构为被告提起行政诉讼。

---

〔49〕 参见张金平：《跨境数据转移的国际规制及中国法律的应对》，载《政治与法律》2016年第12期，第140—142页。

〔50〕 关于个人信息出境安全评估的具体规定，参见《个人信息和重要数据出境安全评估办法（征求意见稿）》和《信息安全技术 数据出境安全评估指南（征求意见稿）》。

〔51〕 按《消费者权益保护法》第34条的规定，若消费者与经营者之间发生了个人信息权益的争议，即可向有关行政部门进行申诉。但是，在《网络安全法》中，应当及时受理和处理关于网络信息安全的投诉和举报的主体为网络运营者，网信部门和有关部门仅对此进行监督检查（参见《网络安全法》第49条）。

再次，协调行政处罚和刑事责任之间的关系。针对侵害个人信息权利的行为而言，只有达到了“情节严重”的程度，才会落入《刑法》第253条之一“侵犯公民个人信息罪”的规制范围。但是，本罪属于非亲告罪，受害人不得提起刑事自诉。由此可见，个人信息的刑法保护不能完全取代行政执法机制。对于侵害个人信息的行为，即使没有达到入罪的程度，受害人仍有进行检举和投诉的权利。

最后，明确因同一侵害行为承担不同责任时的处理规则。在监管对象因侵害个人信息的同一行为同时承担民事责任和行政责任、刑事责任时，其财产不足以支付全部赔偿的，为了实现保障私权的目的，责任人应当先承担民事责任。

五、结　　语

在现代社会中，大数据等技术和商业的迅猛发展，使得个人信息的利用在范围与效率上达到了前所未有的程度。《民法总则》第111条已经迈出了个人信息保护重要的一步，作为单行法的“个人信息保护法”也在2018年9月10日被列入十三届全国人大常委会的第一类立法规划。这意味着，民法典分编与单行法中的个人信息保护制度构建将是未来立法的重点课题。

行政监管是个人信息保护制度的重要内容。但是，由于低层级、多头化和分散式等原因，我国目前的监管设计无法担当起确保个人信息权利保护和法律规范落实的重任。未来的立法应当采用专章（节）来规定“个人信息保护的监管”，设立国家层面的“个人信息保护委员会”，明确规定其监管目标、组织地位、职权范围、监管措施和法律责任，协调与其他保护程序之间的关系，不断夯实个人信息保护的第三大支柱，从而充分应对信息科技兴起带来的法律挑战。

Abstract In the age of big data, personal information becomes increasingly important. As the third pillar of personal information protection, the construction of the vertical regulation system is as important as the establishment of horizontal rights and obligations. However, due to the lack of top-level design and the limitation of decentralized legislation, the present personal information protection regulation in China has many problems, such as weakened objectives, scattered subjects, weak measures and fuzzy procedures, which seriously hamper the improvement of the level of personal information protection. Therefore, facing the legal challenges posed by emerging technologies and the demand for a complex balance of interests, the future legislation should clarify the main regulatory objectives, establish a unified and independent regulatory organization, upgrade its professional and administrative level, specify regulatory measures, and coordinate the relationship between different protection laws and procedures.

Keywords Personal Information Protection, Administrative Regulation, Regulatory Organization, Regulatory Goals, Regulatory Measures

（责任编辑：蒋红珍）