# 《民法典》时代个人信息权的国家保护义务

赵　宏

**摘　要**：《民法典》虽未对个人信息予以权利化处理，但却在私法保护之外，纳入了公法保护，由此将个人信息保护提升至全新高度。个人信息的公法保护框架可具体拆分为国家的消极义务和积极义务两个方面，前者在于防堵国家对于个人信息的无限度收集和不当使用；后者揭示在个人面对与其地位不对等的信息控制者时，国家需承担的介入和保护义务。上述双重义务框架在《个人信息保护法（草案）》中已初现端倪，《个人信息保护法（草案）》也在吸纳欧盟经验的基础上，广泛纳入了公权机关在信息保护中的责任，但该草案的规定还相对粗糙，在上述双重义务构架下，个人信息的公法保护如何展开，还需借助数据法的原理和域外数据立法与实践进行细致讨论。

**关键词**：个人信息权；个人信息的公法保护；国家的消极义务；国家的积极义务

［中图分类号］D923　　［文献识别码］A　　［文章编号］2096-6180（2021）01-0001-20

## 引言

为因应大数据时代下对个人信息的保护，2020 年 5 月 28 日颁布的《中华人民共和国民法典》（下称《民法典》）在第 111 条中明确申明，“自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息”。这一规定对此前散见于《中华人民共和国刑法修正案（七）》〔1〕《中华人民共和国侵权责任法》〔2〕《中华人民共和国消费者权益保护法》〔3〕《中华人民共和国网络安全法》（下称《网络安全法》）〔4〕与《全国人民代表大

［作者简介］赵宏，法学博士，中国政法大学法学院教授。

［基金项目］中国政法大学青年教师学术创新团队项目。

〔1〕《中华人民共和国刑法修正案（七）》在第 253 条增加“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”两项罪名。

〔2〕2009 年颁布的《中华人民共和国侵权责任法》率先在民法领域纳入“隐私”概念，该法第 2 条第 2 款申明，“本法所称民事权益，包括……隐私权”，第 62 条又规定，“医疗机构及其医务人员应当对患者的隐私保密。泄露患者隐私或者未经患者同意公开其病历资料，造成患者损害的，应当承担侵权责任”。

〔3〕2013 年修订的《中华人民共和国消费者权益保护法》第 29 条第 1 款规定，“经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意”。

〔4〕2016 年颁布的《中华人民共和国网络安全法》第四章为“网络信息安全”，其中第 40 条明确规定，“网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度”。

会常务委员会关于加强网络信息保护的决定》[5]等法律规范中的信息保护规定进行了阶段性汇总，也将个人信息保护提升到全新高度。

但《民法典》仅申明“自然人的个人信息受法律保护”，而并未像前款“隐私权”一样，将个人信息保护作权利化处理。[6]因此很多学者指出，《民法典》对于个人信息的保护仍旧有所保留。[7]仔细品读《民法典》的立法说明和背景资料大致可得，《民法典》采用上述处理方式的用意主要在于：其一，信息权作为一类新型权利，其范畴、意涵与定位至今都存有较大争论，因此不宜在《民法典》中过早框定，而应交由专门的个人信息保护法处理；其二，如果将个人信息予以权利化处理，在此项权利边界未明的情况下，容易导致个人的信息独占影响数据流通。[8]

尽管未将个人信息予以权利化处理，但《民法典》却已搭建起个人信息保护的基本制度框架，包括个人信息的界定，处理个人信息的原则要件、信息主体与信息处理者之间的权利义务关系[9]等。尤其值得一提的是，因为《民法典》在第111条指出，个人信息保护指向“任何组织与个人”，“任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息”，此处的“任何组织或者个人”当然包含国家公权机关，故《民法典》虽然是私权的汇总，却同样纳入了对个人信息的公法保护。[10]从这个意义上说，上述规定填补了此前我国法制整体对于个人信息公法保护的缺漏。

新近提交第十三届全国人民代表大会常务委员会第二十二次会议审议的《中华人民共和国个人信息保护法（草案）》（下称《个人信息保护法（草案）》）中，同样在“总则”第11条写明，“国家建立健全个人信息保护制度”。其第二章“个人信息处理规则”专节处理“国家机关处理个人信息的特别规定”[11]，第六章更细致规定“履行个人信息保护职责的部门”。这些规定与《个人信息保护法（草案）》中有关私人信息处理主体的规定相互并置，可说确立了我国在个人信息保护领域

〔5〕2012年通过的该项决定明确规定，“国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息”。

〔6〕伴随数据法的发展，“隐私权”和“信息权”已被普遍作区分处理。“隐私”最初意指不愿为他人知悉的信息秘密，之后又覆盖至自然人享有的私人生活安宁和私密生活空间。《民法典》亦采取了一般的界定方式，认为“隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息”；而“个人信息”依《民法典》的规定则是“以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息”。“个人信息”的范畴中包含了但又不限于“隐私信息”。

〔7〕王利明主编：《中华人民共和国民法总则详解》，中国法制出版社2017年版，第465页。

〔8〕王晨：《关于〈中华人民共和国民法典（草案）〉的说明——2020年5月22日在第十三届全国人民代表大会第三次会议上》，载《全国人民代表大会常务委员会公报》2020特刊，第191－192页；王利明主编：《中华人民共和国民法总则详解》，中国法制出版社2017年版，第465页。

〔9〕参见《民法典》第1034－1036条。

〔10〕尽管《民法典》的信息保护规范在很大程度上是对此前《网络安全法》的照搬和汇总，但《网络安全法》的规制对象却主要局限于“网络运营者”，即网络的所有者、管理者和网络服务提供者。从该法第9条要求网络运营者开展经营服务活动需要“接受政府和社会监督”的语义判断，“网络运营者”并不包含政府机关，因此，《网络安全法》中的有关个人信息收集和适用的相关规定并无法直接适用于国家机关。

〔11〕《个人信息保护法（草案）》第二章第三节“国家机关处理个人信息的特别规定”从第33条至第37条共5条，分别涉及国家机关处理个人信息的一般规则，国家机关为履行法定职责处理个人信息的基本规范、“告知同意”原则对于履职行为的适用与例外、国家机关公开和向他人提供个人信息的禁令和例外、国家机关向境外提供个人信息的基本要求等。

公私协力、合作共治的基本格局，也彻底化解了此前有关“数据立法的公私之争”。[12]

在私法保护之外，强调个人信息的公法保护固然重要，但如何确立个人信息权公法保护的圭臬，却存在诸多难题。个人信息的公法保护首先涉及对国家无限度收集和不当使用个人信息的防堵，但在处理这一命题时，又需要在数据流通、数据开发所追求的公益与个人信息权所维护的私益之间进行权衡，这一难题在大数据时代下并无法轻易化解。在此次抗击新冠肺炎疫情中，该点表现得尤为突出。从最初个别地方政府为阻却疫情传播曝光返乡人员名单而引发众怒，至后来政府在公布确诊患者的住址信息和行踪信息时的详尽程度之争，再至学者们对健康码被泛化使用的担忧，以及对个别地区启动人脸识别技术后引发的诘难，本质上反映的都是这一问题。《民法典》在规范信息主体与信息处理者之间的权利义务关系时指出，如果是“为维护公共利益”而处理个人信息，则行为人不承担民事责任，其目的是通过这一免责条款来达到对“保护个人信息与维护公共利益之间关系”的合理平衡。但“公共利益”一词可说是公法中最大的概念谜团，其在一定程度上可以正当化国家公权机关收集和使用个人信息的行为，却很难对此种数据处理行为予以有效规制，更不容易调控信息保护与数据流通之间的矛盾。因此，对于国家公权机关可因何种公益追求而对个人信息予以收集和使用需要更细致的分析，对这种行为的限度也需更深入的挖掘。此外，个人信息权的公法保护所强调的并不只是对国家无限度收集和不当使用个人信息的防御，还包含个人信息权在面临同为私主体的第三人侵害时国家的积极介入义务。但国家对此积极义务的履行，本质上又是对原本应由私法调整的以“用户—平台”为代表的民事关系的干预和渗透。公权介入的正当性基础何在，国家此时又如何选择监管手段，如何调配私人自治与国家干预之间的比重与关系，这些问题亦须在个人信息权公法保护的整体框架下予以思考。

基于上述思考，笔者首先从个人信息权的传统保护路径和复杂属性出发，尝试在将个人信息权塑造成基本权利的基础上，以基本权利教义学为参考，廓清个人信息权公法保护的基本框架，进而以《民法典》和《个人信息保护法（草案）》为规范基础，探讨这一保护框架下所涉及的具体问题。笔者尝试在《民法典》时代下，梳理出个人信息权公法保护所涉及的核心问题和思考难点。

## 一、信息权的保护路径与复杂属性

在数据时代，个人信息是个体在社会中标识自己，并与他人建立关联的必要工具。个人信息若被不当收集和使用，将严重危及个体由信息所组成的数据人格，进而贬损其人性尊严。正是基于上述共识，各国都已普遍展开对个人信息的严格保护。但值得关注的是，与同时兴起的其他权利保护需求不同，尽管人们对信息权的保护必要并无异议，但对信息权的属性判定却自始都存在认识分歧。

### （一）信息权的属性与保护路径之争

典型的代表性意见之一是将信息权作为财产权来处理。“像保护私有财产一样保护个人数

〔12〕 周汉华：《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 153 页；郭瑜：《个人数据保护法研究》，北京大学出版社 2012 年版，第 245 页；赵宏：《信息自决权在我国的保护现状与趋势前瞻》，载《中国法律评论》2017 年第 1 期，第 147 页。

据”[13]反映的就是这种呼声。这种意见的支持理由除了信息数据的确可以销售并带来经济收益外，还包含了学者希望经由“个人数据的财产化”（propertization of personal data）[14]，以通过财产侵权模式来保护个人数据的考虑。支持个人信息权属于新型财产权的学者，在我国最初不在少数[15]，但这种观点很快被数据人格权的观点所替代。其思考脉络在于，现代数据技术已经将个人降格为硬盘中可被随时调取且分析的数据，通过获得、汇集和整合人们在日常生活中所留存的种种生活轨迹，数据技术已完全能够在短期内描摹出与个人实际人格相似的数字人格。既然数据已然成为个体完整人格的投射，人格权保护就应拓展至个人的数据人格。对个人信息的保护，也成为数据时代下对个体人格权保护的延伸。这种将数据权人格权化的处理为德国首创，之后在欧盟获得普遍认可。[16] 数据人格权的处理为个人信息权提供了人性尊严、个人自治（自我确定和自我展开）的宪法教义学支持，也一举将个人信息权从最初的私权提升至基本权利的位阶序列。

在被提升为基本权利后，个人信息权被描述为个人基于自我确定（Selbstbestimmung）和自我展开（Selbstentfaltung）的自我决定权，其概念和意涵又主要凝结于德国法上的“个人信息自决权”，即“个人具备权利，以自行决定何时并在何种限度内披露其个人生活的事实”。[17] 在被提升为基本权利后，信息权具有了对抗国家的面向，其不仅可以防堵私主体，同样可以防御国家借由对个人信息的无限度收集和违法使用，而对个人生活轨迹予以巨细靡遗的描绘。[18]

与德国的保护路径不同，美国的信息保护虽然也从私人领域扩张至公共领域，却一直是在隐私权的框架下展开。伴随时间演进，德美之间的差异已经渐次相对化。由美国联邦最高法院诸多判决所确认的“宪法隐私权”，本质上就是德国法上“个人信息自决权”的对应，这一概念同样直指国家对个人信息的搜集、储存、利用和公开等行为的合法与正当，隐私权也自此摆脱了私权的偏狭格局，同样被提升至宪法高度。此外，因为美国修订《隐私法》时，将“隐私”的保护对象拓展至“个人被政府机关所掌控的记录系统”，“宪法隐私权”的保障范围也与信息权几无差异。

### （二）“信息权”权利化处理的问题

但无论是将信息权形塑为私法上的财产权还是人格权，抑或按照信息自决权或宪法隐私权的基本权路径对其予以保护，因为受制于传统权利建构模式的影响，信息权都被或多或少地赋予绝对化和个体化的色彩。而这又与数据时代下基于数据自由流通所欲追求的公益和其他法益之间形

〔13〕 丁晓东：《个人信息私法保护的困境与出路》，载《法学研究》2018年第6期，第197页。

〔14〕 郭瑜：《个人数据保护法研究》，北京大学出版社2012年版，第161页。

〔15〕 汤擎：《试论个人资料与相关的法律关系》，载《华东政法学院学报》2000年第5期；洪海林：《个人信息财产化及其法律规制研究》，载《四川大学学报（哲学社会科学版）》总第146期；刘德良：《个人信息的财产权保护》，载《法学研究》2007年第3期；齐爱民：《论信息财产的法律保护与大陆法系财产权体系之建立——兼论物权法、知识产权法与信息财产法之关系》，载《学术论坛》2009年第2期。

〔16〕 2000年《欧盟基本权利宪章》第8条规定，“人人均有权享有个人数据的保护，个人数据只能基于特定目的，基于当事人同意或者其他法律依据而被公正地处理”。

〔17〕 BverfGE 65, 1.

〔18〕 赵宏：《信息自决权在我国的保护现状与〈个人信息保护法〉的趋势前瞻》，载《中国法律评论》2017年第1期，第160页。

成张力。以信息自决权为例，其意涵是“个人对其一切具有识别性的个人信息的收集、处理和利用均享有决定权和控制权”，也因此要求信息主体要对数据的获取、处理过程完全知情和充分参与。这就导致个人对数据的自决与控制自始就包含一种绝对化的趋向。知情同意最初作为调控信息保护的首要原则，也正是基于个人对信息的控制要求。德国联邦宪法法院在最初提出信息自决权概念时，已经意识到这一问题，并尝试通过指出“信息自决权并非无限，对其自身信息，个人并不具有任何绝对或无限的控制”，“为了迫切的公共利益，个人在原则上必须接受对其信息自决权的某种限制”，来对其绝对化趋向予以缓解。〔19〕与德国信息自决权思路一脉相承的欧盟《通用数据保护条例》（GDPR）同样申明，“保护个人数据的权利不是一项绝对权利，应考虑其在社会的作用，并根据比例原则与其他基本权利保持平衡”。

因为信息自决权的推导是从个体的人格自治出发，这就导致其从根本上还是带有传统权利个体化的、排他的和积极的支配属性。〔20〕但在数据时代，一方面能够对个体身份和个性特征予以识别的信息海量产生，数据技术的疾速发展也使对个体的识别更加便利、精准和全面；另一方面数据时代的红利，也确须尽可能多地鼓励数据处理者对信息进行分析识别，推进数据流通和数据交易，进而实现社会发展。据此，如果沿用传统权利的思考框架和保护模式，强调个人对于数据的绝对支配和过高的同意要求，显然就会妨碍数据处理和数据流通，并最终丧失数据时代的红利。这一问题反映于法学领域就表现为：越来越多的学者开始主张，“个人信息只是一种可以识别某个人的事实或记录，并不当然地应该由个人拥有或控制”，即数据本身具有“公共性和可共享性”。〔21〕这种公共性表现为：“目前个人数据在定义上几乎被视为公共领域的组成部分，是可以广泛获得和使用的，无论是从实践还是从法律目的上，个人数据均处于公共领域。”〔22〕而且，在个人信息之上所附着的不仅有自然人的私益诉求，还有公共管理、国家安全等公益属性。如果仅因数据和个人存在联系或具有识别性，就赋予个人对个人数据的排他性控制权，为私人所专有独断，不仅与共享要求不符，也有失法律正当。其最终结果只能是产生“数据壁垒”和“信息孤岛”。〔23〕如何调试大数据发展与个人信息保护，是数据时代下的最大挑战。〔24〕如序言所述，《民法典》仅对个

〔19〕 BverfGE 65，1.

〔20〕 高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018 年第 3 期，第 240 页；纪海龙：《数据的私法定位与保护》，载《法学研究》2018 年第 6 期，第 264 页。

〔21〕 高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018 年第 3 期，第 247 页。

〔22〕 高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018 年第 3 期，第 248 页。

〔23〕 Corien Prins, *Property and Privacy: European Perspectives and the Commodification of Our Identify*, 16 Information Law Series 223 (2006). 经济学上也认为数据和信息不同于其他生产要素，具有公共产品才具有的非排他性、非独占性的特点。但值得关注的是，很多学者在个人信息的共享性上走得更远，认为个人信息立法的首要目的就在于促进共同利益而非私人利益，因此应弱化自然人对信息的占有，允许各方对信息的收集、分析和使用。但这一观点却有待商榷。参见彭诚信：《数据利用的根本矛盾何以消除——基于隐私、信息与数据的法理厘清》，载《探索与争鸣》2020 年第 2 期，第 79－85 页。

〔24〕 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.

人信息保护进行框架化处理，并未如部分学者所主张的直接将个人信息进行权利化处理，反映的也正是“合理平衡保护个人信息与维护公共利益”的难题。

综上，信息权的复杂性要求我们不能用传统权利的观点去认识和框定这一新兴权利；但反过来，如果我们仅因这一原因就刻意回避权利话语，在未来仍旧还是以此前数据安全、风险防范的思维方式去思考数据保护的问题，也无法因应数据时代下数据保护的需要。[25] 正是基于这一背景，尽管《民法典》对信息保护未作权利化处理，但新近提交审议的《个人信息保护法（草案）》却是在借鉴欧盟的经验基础上，“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，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、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”。[26] 在有关《个人信息保护法（草案）》的立法说明中，“制定个人信息保护法是进一步加强个人信息保护法制保障的客观要求”，被排在所有立法目的之前予以强调。该法第2条已明确出现“个人信息权益”的提法，第四章则体系化地列举“个人在个人信息处理活动中的权利”，包括个人对其信息处理的知情权、决定权、查阅权、复制权、更正权、补充权、删除权等，上述规定对应第五章“个人信息处理者的义务”，塑造出个人信息权作为“权利束”的完整图像。但同时值得玩味的是，《个人信息保护法（草案）》第四章的标题为“个人在个人信息处理活动中的权利”，而非“个人信息权利”，此处的表达差异和对权利的前缀限定，同样反映出立法者基于“维护网络空间良好生态”“促进数字经济健康发展”[27] 等其他法益考虑，而对信息权所作的区别于传统权利的差异化处理。

## 二、信息权公法保护的基本架构和国家的双重义务

以德国基本权利教义学为参考，公法对于基本权利的保护主要通过如下方式展开：首先是国家的消极义务。消极义务的基础在于基本权利的防御权（Abwehrsrecht）功能，即所有的基本权利构筑出一个私人生活领域，在此领域中排除国家的不当干预，而国家为此所承担的义务也仅是对此私人自由和自治空间予以尊重、保持克制、不予犯进。其次是国家的积极义务。积极义务要求国家必须积极作为以帮助和促进个人基本权利的实现，积极义务先是通过个人的给付请求权获得表现，此外在个人基本权利受到第三方影响时，国家还负有义务为其提供保护。后者在德国法中被归纳为国家的保护义务（Staatliche Schutzpflichtung）。[28] 概言之，国家对基本权利的积极义务主要由给付与保护来构成。上述法教义框架对于我国宪法学同样影响深远，我国在2004年修宪

〔25〕 在《民法典》颁布之前，我国在数据保护领域最重要的立法为《网络安全法》，但该法的目的并非确立个人的数据权利，而首先是“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”。

〔26〕 周汉华：《探索激励相同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。

〔27〕《全国人大常委会网络安全法执法检查报告建议 加快个人信息保护法立法进程》，载中国人大网，http://www.npc.gov.cn/zgrdw/npc/zfjc/zfjcelys/2017-12/25/content_2035344.htm，2020年12月15日访问。

〔28〕 Hartmut Maurer, Staatsrecht Verlag C, H, Beck Muenchen 2003, S. 274.

时，将“国家尊重和保障人权”规定于《中华人民共和国宪法》第 33 条第 3 款中。这一条款不仅被宪法学者延伸解释为我国基本权利的概念性条款〔29〕，宪法学者还比对德国基本权利教义的上述结构，从“尊重”和“保障”用语的差异与并置中推演出国家对于基本权利的双重任务，即“尊重”代表了国家对基本权利的消极义务，而“保护”则对应国家的积极义务。〔30〕

（一）国家对于信息权的双重义务

既然信息权已被提升至基本权序列，那么将上述思考模式适用于信息权的公法保护，国家为此承担的义务就同样可拆分为两个方面：首先是消极义务。这种义务在信息权保护中表现为个人基于信息自决免受国家对其信息的无限度收集和不当使用。消极义务的目标在于防堵国家在数据时代下，借由数据调取和数据整合技术，产出部分或是几乎完整的“个人轮廓”，并由此对公民的私人空间和自决能力予以削减。其次是积极义务。在积极义务方面，因为对信息权的保护几乎并不需要国家的积极给付，这一部分就着重体现为个人作为信息主体，面对与其地位不对等的其他信息控制者时，国家须承担的介入和保护义务。

在实践中，除国家为公共利益和平衡其他法益而收集、使用个人信息外，个人数据的另一重要收集和控制者还包括以互联网平台为代表的私主体。对于这些私人信息控制者，数据就是生产要素和行动指引，其可通过数据揭示的相关性，提前预测信息主体和社会的各种需要，从而获得巨大的经济收益，这也是私主体收集和使用个人信息的最大动因。但因为这些私人信息控制者在数据技术上的绝对优势，作为个人的信息主体几乎很难通过传统的私法侵权模式予以对抗，由此便要求国家通过行业监管、执法威慑、责任追究等方式，积极介入以“用户—平台”为代表的私法关系中，以确保个人信息同样免受其他私人的非法收集和不当使用。

上述公法保护的基本架构如图 1 所示。

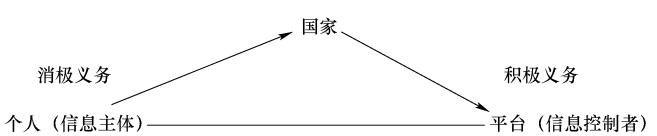


**图 1　公法保护的基本架构**

回溯至《个人信息保护法》的起草过程，公法保护和私法保护对于数据权的全面保护虽都不可或缺，但在立法过程中，还是出现过个人信息保护的重心究竟落脚于行政法保护还是民法保护的争论。这一争议又延伸出个人信息的保护模式以及政府与个人责任分配之争。〔31〕但大数据时代下的数据保护难题却证明，个人信息保护已经远远超出了公私法二分的传统格局，单独倚重任何

〔29〕 韩大元：《宪法文本中的人权条款的规范分析》，载《法学家》2004 年第 4 期，第 12 页。

〔30〕 张翔：《基本权利的体系思维》，载《清华法学》2012 年第 4 期，第 31 页。

〔31〕 有关信息保护应落脚于公法保护还是私法保护的争论，参见赵宏：《信息自决权在我国的保护现状与〈个人信息保护法〉的趋势前瞻》，载《中国法律评论》2017 年第 1 期，第 150 页。

一个方面都会有所欠缺，而真正有效的治理模式必然是一种多元并行的综合框架。

（二）《民法典》与《个人信息保护法（草案）》中的双重保护架构

上述观念也已在《民法典》中呈现端倪。但从《民法典》的具体规定来看，其虽纳入了信息权的公法保护，其中规定的信息处理的核心法则，例如“合法、正当、必要原则，不得过度处理”，以及相关的条件性指引包括知情同意原则、公开原则、目的明确与受目的限制等〔32〕，却都同样适用于作为数据控制者的国家和私主体。从这个意义上说，除了提供了个人信息保护的基本制度框架外，《民法典》对于公法保护和私法保护如何并置发展，尤其是国家和私主体在信息收集和处理方面虽然遵守同样的原则指引，但具体适用时是否存在差异，并未作更详尽的说明和提示。

最近提交审议的《个人信息保护法（草案）》除延续了《民法典》公私并置的保护格局外，在具体展开上显然是汲取了德国与欧盟的有益经验，因此，国家在数据保护中的双重义务构造同样呈现于这部草案中。《个人信息保护法（草案）》在第一章“总则”第4条列举了个人信息的一般范畴，第5～9条列举了信息收集处理的基本原则〔33〕后，在第二章“个人信息处理规则”中系统描画了个人信息处理的一般规则，本章第三节则专门规定“国家机关处理个人信息的特别规定”，由此突出对国家机关的特殊规制。此外，《个人信息保护法（草案）》明确吸收了欧盟《通用数据保护条例》的模式，在第六章确立了专门的信息保护机构。根据该法第56条的规定，我国专门负责统筹协调个人信息保护工作并履行相应监督职能的部门为国家网信办。本章还对网信部门在此领域的基本职责、权限划分、作用手段和处理机制等问题进行了细致规定。由此可见，我国的《个人信息保护法（草案）》最终还是在强调行业自律的基础上，明确纳入了公法保护的框架和内容。因此，上述由德国基本权利教义学所延伸出的信息权公法保护架构，对我们思考个人信息的公法保护问题无疑具有重要参考价值。下文就以此架构为思考基础，以《民法典》和《个人信息保护法（草案）》为规范线索，并以数据法的一般原理和域外经验为借鉴，对国家在履行数据保护方面的双重义务时所涉及的核心问题进行讨论和总结。

## 三、消极义务下的数据公法保护规则与问题

上文论及数据时代下私主体在信息收集和使用方面的经济动因，对于国家而言，数据收集和处理作为治理手段同样重要且极富吸引力。从我国的既有实践看，如果说最初国家利用采集指纹、身份登记、视频监控、实名注册等数据处理技术，所欲追求的只是在城市化疾速发展的背景下，保障社会稳定、打击犯罪、强化治安等目的，那么现在的数据处理技术早已使数据跃升为国家基础性的战略资源，大数据发展也成为国家发展战略的重要构成。2015年国务院发布的《促进大数

〔32〕 参见《民法典》第1035条。

〔33〕《个人信息保护法（草案）》第5－9条规定的信息收集和处理的一般原则包括合法、正当原则、诚信原则、知情同意原则、目的明确原则、限制利用原则、公开透明原则、信息准确原则等。个人信息和数据权作为“权利束”的提法，参见闫立冬：《以“权利束”视角探究数据权利》，载《东方法学》2019年第2期。

据发展行动纲要》就指出，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。〔34〕以此次抗疫为例，数据收集、整理和排查自始就是政府抗疫工作的关键，其适用也大大提升了抗疫工作的针对性和实效性。〔35〕因此，我们在数据技术疾速发展的背景下，论及数据流通所要维护的“公共利益”，其内涵除了传统的公共安全外，还直指“数字中国”“数字政府”这些提法背后所倡导的全新公共治理技术，以及借由数据治理所欲达到的“推动政府治理精准化、推进商事服务便捷化、加快民生服务普惠化”〔36〕的公共目标。

因为政府治理与数据技术结合的不断拓展，由“物尽其用”延伸出的“数尽其用”，便成为支配政府“数据治理”的基本准则。反映在近年的公共政策推进上，我国最早推行电子政务时就着力于数据库建设。〔37〕之后伴随政府信息公开的深入，又提出政务部门不仅要“主动为企业和公众提供公益性信息服务”，还要“积极发展信息资源市场，发挥市场对信息资源配置的基础性作用”。〔38〕这些早期的政策探索都为此后政府进一步开放政府数据，制定大数据战略，推进数据产业发展奠定了基础。迄今，“政府数据开放共享、数据产业创新发展和安全保证”更被总结为政府大数据发展的三大任务。

“数尽其用”强调的是在公共政策上国家对数据技术的积极利用和对数据治理的持续推进，但将这些举措放在法教义的框架下检视，所涉及的首要问题却是：国家的数据治理最终都会落脚于每项具体的数据收集和处理行为，而当国家公权机关以“公共利益”为名去收集和处理个人信息时，其法定界限何在？尤其是当我们用数据法中的一般原则去约束国家的信息收集和处理行为时，又会面临何种问题，需要作出何种调试？《民法典》和《个人信息保护法（草案）》在规定个人信息的处理原则时，都纳入了合法正当、必要（比例）、有限使用、知情同意、目的明确与目的限制等数据法的核心原则。下文就对这些原则对于公权机关的具体适用问题进行逐项讨论，并从中归纳出国家在履行信息保护的消极义务时所涉及的问题。

### （一）合法正当

“合法正当”既针对数据收集和处理的目的，也针对其手段。这一要求除规定于《民法典》第

〔34〕《国务院印发〈促进大数据发展行动纲要〉》，载中国政府网 2015 年 9 月 5 日，www.gov.cn/xinwen/2015-09/05/content_2925284.htm。

〔35〕以最新爆出的青岛群体性疫情传播为例，青岛在疫情爆出 5 日内就完成 1 082 万份新冠病毒核酸检测，并确定造成传统的零号病人和疫情源头，成功阻却疫情的社区传播。这与大数据使用密切相关。参见《青岛疫情源头查明，外媒集体沸腾：中国人，太狠了!》，载搜狐网 2020 年 10 月 23 日，https://www.sohu.com/a/426667063_120877413。此前的北京新发地疫情在爆出后也很快得到控制，同样与大数据使用密切相关。

〔36〕《李克强在全国深化“放管服”改革转变政府职能电视电话会议上的讲话》，载中国政府网 2018 年 7 月 12 日，http://www.gov.cn/xinwen/2018-07/12/content_5305966.htm。

〔37〕《国家信息化领导小组关于我国电子政务建设指导意见》（中办发〔2002〕17 号）即提出要建设人口基础信息库、法人基础信息库、自然资源和空间地理信息资源库、宏观经济数据库。“十二五”国家政务信息化工程规划又增加了“文化信息资源库”，“十三五”又将文化库和宏观库替换为社会信用信息库。

〔38〕参见《中共中央办公厅、国务院办公厅关于加强信息资源开发利用工作的若干意见》（中办发〔2004〕34 号）。

1035条第1款中，“处理个人信息的，应当遵循合法、正当……原则”，还在本款第4项中被强调，处理个人信息应“不违反法律、行政法规的规定和双方的约定”。在《个人信息保护法（草案）》第13条中同样包含了更细致的国家机关处理和利用个人信息的“合法正当”说明。合法正当原则的纳入以及正当理由的列举也排除了自《网络安全法》生效以来，“知情同意”作为信息收集唯一合法性基础的操作准则。

一般而言，国家公权机关收集和处理个人信息的合法正当目的主要在于公益维护。上文所具体列举的“履行法定职责或者法定义务”“为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全”等规范表述，都可被列入此类范畴。但从数据实践来看，如果仅是概观的、抽象的“公共利益”，并无法正当化公权机关所有的数据收集行为，因为概括性的公益目的几乎无法为限制公权机关不当收集和使用个人信息划定任何界限。而且，抽象的“公益需求”也不能在与个人的数据权衡量时被赋予绝对的、永恒的优先性。据此，如果公权机关在公共利益和个人的数据私益发生冲突时，以公益为由要求对个人私权予以合理限制，国家机关则应承担对“公共利益”予以具体化框定和说明的义务。唯有对所欲追求的“公益”在具体个人私权中予以详细说明，才便于对公权机关是否滥用数据、是否违反合法正当的要求进行评鉴，也唯有“公益”目的本身是足够清晰和特定的，公权机关才能从这些特定目的出发进行数据收集和使用。〔39〕

事实上，从欧盟的数据实践来看，合法正当作为单独的原则对于防堵公权机关无限度收集和不当使用个人信息其实作用有限，而必须辅以其他原则。因此，即使《个人信息保护法（草案）》将“履行法定职责或者法定义务”“为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全”等列举为收集个人信息的正当目的，但在规范表达上同样会附加“所必需”表达对其限度的限制。而在《个人信息保护法（草案）》第27条关于在“公共场所安装图像采集、个人身份识别设备”的规定中，除要求此类行为必须是“为维护公共安全所必需”，还规定必须“遵守国家有关规定，并设置显著的提示标识”。

### （二）目的明确与目的限制

“目的明确与目的限制”一直也是数据保护的核心原则。这一原则首先要求数据控制者明确收集、使用个人信息的目的，禁止其为未来不特定的目的考虑收集、使用个人信息；其次则是约束信息控制者对信息的使用受所明示的目的限制，而不得将所搜集的信息作法定目的外使用。〔40〕

除《民法典》第1035条明确列举目的明确与目的限制原则外，这一原则虽然未单独落实于《个人信息保护法（草案）》的具体条款中，但其要求却贯穿于第二章“个人信息处理规则”中，例如

〔39〕此前发生的苏州政府推行“文明码”事件中，政府后来提示说，文明码的信息收集和使用是为了提升“社会整体的文明指标”，但这种宽泛的“公益目的”设定，却无法为限定政府的数据操控提供帮助，原因是有关社会文明的事项包罗万象，个人所有的数据也都直接或间接与此目的相关。参见赵宏：《被数据操控的人生》，载澎拜新闻网 2020 年 9 月 17 日，https://www.thepaper.cn/newsDetail_forward_9217083。

〔40〕Spiros Simitis, Die informationelle Selbstbestimmung-Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, S.395.

第 18 条规定，“个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言向个人告知下列事项：……（二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；……”；第 22 条规定，“个人信息处理者委托处理个人信息的，应当与受托方约定委托处理的目的、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托方的个人信息处理活动进行监督。受托方应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息……”；第 24 条第 1 款规定，“个人信息处理者向第三方提供其处理的个人信息的，应当向个人告知第三方的身份、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收个人信息的第三方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。第三方变更原先的处理目的、处理方式的，应当依照本法规定重新向个人告知并取得其同意”。

目的明确与目的限制在适用于国家和私人主体上并无明显差异，但这一原则在数据实践中却常常被国家公权机关突破。以此次抗疫为例，尽管 2020 年中央网络安全和信息化委员会办公室印发的《关于做好个人信息保护利用大数据支撑联防联控工作的通知》中强调，“为疫情防控、疾病防治收集的个人信息，不得用于其他用途”，但从各地的健康码的使用情况来看，却都存在不同程度上超越最初的目的设定而被逐渐泛化使用的趋向。很多政府甚至将简单的健康评价与公众本应享有的公共服务建立关联，并将其作为是否对相对人予以赋权或设限的依据〔41〕，这显然背离了目的限制的基本要求。避免上述做法的首要手段在于，应尽可能禁止公权机关使用模糊、宽泛的语词表述其约定目的，进而为其未来扩大收集和使用个人信息提供可能。以欧盟 GDPR 为鉴，其在规定目的明确时专门设定了三项判定基准：其一，特定（specified），所谓特定即目的应当在不迟于收集个人信息时确定下来，而且对目的的描述必须提供足够的细节，使之具有辨识度；其二，明确（explicit），即目的特定化后，还应当明白无误地展现出来，应尽力确保信息主体、信息控制主体以及利用个人信息的第三方都能够对该目的具有一致理解；其三，合法（legitimate），即公权机关对个人信息的处理必须公平且依法进行，不得以非法目的收集个人信息。〔42〕这种对于“目的明确”的细致要求在很大程度上避免了放任目的的空泛化。

在目的明确与目的限制原则的公法适用上，还涉及如何平衡个人信息保护与基于公益目的的大数据开发利用之间的矛盾问题。单个信息的交换价值微乎其微，唯有信息聚合和数据利用才能产生出强大的分析价值。此外，因为网络技术的迅疾发展，信息主体和信息控制主体在信息收集时可能都无法充分预见信息在未来的可能价值。此时如果一律禁止个人信息用于其他目的，势必会造成资源浪费。由此，就要求在严格的“目的限制”之下应留存一定的例外。欧盟 GDPR 将“为公共利益、科学或历史研究或者统计目的而（对数据进行的）进一步处理”，作为“目的限制”的例外。〔43〕欧盟指令也同时允许基于其他“额外目的”而对个人信息的“适当性使用”。对“适当

〔41〕《苏州文明码引争议》，载腾讯网 2020 年 9 月 6 日，https://new.qq.com/omn/20200906/20200906A0HEBC00.html?Pc。

〔42〕梁泽宇：《个人信息保护中目的限制原则的解释与适用》，载《比较法研究》2018 年第 5 期，第 22 页。

〔43〕参见 GDPR 第 5 条。

性使用”的判断依赖于如下标准：其一，信息收集目的与预期进一步处理目的之间的关联；其二，个人信息被收集时的情形，尤其是信息主体与控制者之间的关系；其三，个人信息的性质；其四，预期进一步处理给信息主体可能造成的后果；其五，加密或匿名化保障措施的存在。〔44〕但欧盟的上述做法同样引发争议。反对者认为，额外目的使用的允许，会通过功能渐变逐渐掏空目的限制原则。〔45〕这种隐忧也的确提示了放宽目的限制的可能问题。

在《个人信息保护法（草案）》出台前，亦有学者呼吁将“为防止危害国家安全和公共安全所必要的；为反恐怖活动、反恐怖融资和反洗钱等所必要的；侦查机关进行刑事侦查所必要的；税务机关为防止逃税、骗税等行为损害国家税收利益所必要的；为支持学术研究工作或统计项目而进行的个人信息比对；为得到统计资料……”〔46〕等，作为国家公权机关可进行信息比对的理由，由此从另一侧面规定了“目的限制”的例外。但最终提交审议的草案中并未包含突破目的限制使用个人信息的例外。因此，从目前的《个人信息保护法（草案）》来看，其并未允诺在收集目的之外的其他延伸目的的使用。无论是公权机关还是私人主体如果嗣后欲突破目的限制，都必须重新获得信息主体的同意。但由此产生的为因应数据开发利用的需要，而对“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”〔47〕，豁免或克减适用目的限制原则的问题，就有待于国务院相关部门再出台细则予以规范。

（三）知情同意

在欧盟和德国有关信息权的保护框架下，信息权被视为人格权的延伸，是基于个人自治对个人信息的自我控制，因此，“知情同意”一直被作为信息收集和处理的首要法则，这一原则确保了信息主体对于个人信息收集和使用过程的完全知情和充分参与，也体现了个人对于信息的自决与控制。

欧盟早在1995年的《关于个人数据处理保护与自由流动指令》（95/46/EC，下称95指令）中就将“数据主体同意”视为个人数据处理取得合法性的首要基础，而且“同意要求”的广泛存在，不仅及于作为数据控制者的私人机构，也及于公共机构；不仅及于对数据的采集，也及于对数据的传播、加工或其他处理行为。〔48〕但将“知情同意”作为数据处理的首要法则，并贯穿于数据采集处理的全部过程，势必会抬高数据处理门槛，阻碍数据自由流通。〔49〕鉴于此，欧盟GDPR尽管

〔44〕梁泽宇：《个人信息保护中目的限制原则的解释与适用》，载《比较法研究》2018年第5期，第24页。

〔45〕Judith Rauhofer, *What Do the Proposed Changes to the Purpose Limitiation Principle Mean for the Public Bodies' Rights to Access Third-Party Data?*, 28(2) International Review of Law, Computers & Technology 144, 146 (2014).

〔46〕周汉华：《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9页。

〔47〕周汉华：《探索激励相同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288页。

〔48〕郭瑜：《个人数据保护法研究》，北京大学出版社2012年版，第152页。

〔49〕相比之下，美国在数据处理上并不以“个人同意”作为基本前提，而是认为个人数据是一种自然存在，只要是为了合法目的即可收集和适用，无须事先征得个人同意，唯有对于特殊领域的特定类型的个人数据或针对这些数据的特殊处理方式才需要征得数据主体的同意。

同样以“知情同意”为基础，建构了用户的访问、查询、更正、删除、撤回、限制、拒绝等个人信息自决权体系，但同时也规定了广泛的例外情形，由此在很大程度上缓和了严苛适用这一原则所带来的负面效果。从研究现状看，对知情同意原则的反思与改进一直都是数据法的重点，其目标也基本积聚于如何破除数据实践中知情同意的简单化、概括化与机械化偏差，并在提升这一原则的有效性之余，同样为信息流通和再利用预留空间。

具体至公法保护领域，此处须讨论的是，国家作为信息权的公共义务主体和私人的信息控制者在适用“知情同意”原则时具有何种差异。一种典型意见认为，知情同意作为个人信息保护准则并不能直接适用于公权机关。公权机关在执法过程中所获取的个人信息属于“执法隐私”〔50〕，其并非基于用户与平台这类典型的持续性的非对等的信息关系所产生，也不受知情同意原则的约束。理由是，“如果执法机构获取个人信息都需要个人同意，那么个人就会有足够时间与机会藏匿或删除执法所需信息；同样，如果个人对于自身信息具有访问权、纠正权、删除权等权利，那么个人就能利用这些权利破坏执法所需要的信息与证据”，并最终“破坏国家的执法能力”。〔51〕还有意见认为，知情同意只能在平等关系下适用，如果“个人在权力失衡与权力依赖情况下很难保障同意的真实、自愿与自由，只有拥有控制力，能够在不损害个人利益的前提下自由做出并真实表达同意与否的决定，且此决定可以随时撤回时，同意才可成为合法性基础”〔52〕，因此，同意原则并不适用于公权机关。

将视线再转向欧盟 GDPR，该条例在规定“知情同意”时，仅将其作为数据处理合法化的一种情形。与此相对，如果数据处理是“为了保护数据主体或其他自然人的重要利益”“是为了执行公共利益领域的任务或行使控制者既定的公务职权之必要”，“知情同意”就不再适用，其也不再是数据处理的合法前提。〔53〕从这个意义上说，欧盟法的一般观点也是，作为数据控制者的公权机关如在履行既定的公务职权，原则上就不再受制于“知情同意”原则。〔54〕这也意味着，“同意”并非是公权机关进行数据处理的唯一合法性事由，“为履行法定义务或法定职责”同样会为其合法正当性提供证成。

〔50〕 Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 Harward Law Review 1089, 1089 (1972).

〔51〕 丁晓东：《个人信息权利的反思与重塑：论个人信息保护的适用前提与法益基础》，载《中外法学》2020 年第 2 期，第 345 页。

〔52〕 蔡星月：《数据主题的弱同意及其规范结构》，载《比较法研究》2019 年第 4 期，第 78 页。

〔53〕GDPR 第 6 条规定，“处理的合法性 1.仅在适用以下至少一项的情况下，处理视为合法：（a）数据主体同意其个人数据为一个或多个特定目的处理；（b）处理是数据主体作为合同主体履行合同之必要，或者处理是因数据主体在签订合同前的请求而采取的必要措施；（c）处理是控制者履行法律义务之必要；（d）处理是为了保护数据主体或其他自然人的重要利益；（e）处理是为了执行公共利益领域的任务或行使控制者既定的公务职权之必要；（f）处理是控制者或者第三方为了追求合法利益之必要，但此利益与被要求保护个人数据的数据主体的利益或其他权利自由相冲突的除外，尤其是数据主体为儿童的情形下。前款（f）项不适用公权力机构在履行其职责时进行的处理”。

〔54〕《民法典》的处理方式是将国家公权机关为维护公共利益而合理实施的数据处理行为理解为“处理个人信息的免责事由”，参见《民法典》第 1036 条。

在提交审议的《个人信息保护法（草案）》中，同样能够明显看到“知情同意”原则在个人信息处理中的优位性。其第二章“个人信息处理规则”中，第13条第1项明确将“取得个人的同意”作为个人信息处理者处理个人信息的一项合法要件，第14条至第17条则细致规定了有关“同意”的具体意涵。除个人信息处理中的“知情同意”外，第26条和第28条同样将“同意”作为个人信息处理者公开个人信息以及超出公开目的使用合法信息的合法性前提。而在涉及敏感个人信息时，“同意”的要求更会提高，如第30条要求取得个人的单独同意。概言之，《个人信息保护法（草案）》也的确如其说明所说，是“确立以‘告知—同意’为核心的个人信息处理一系列规则”。

但对权重增加的“知情同意”原则是否会同等程度地适用于公权机关，《个人信息保护法（草案）》作了特别规定，其第35条申明，“国家机关为履行法定职责处理个人信息，应当依照本法规定向个人告知并取得其同意；法律、行政法规规定应当保密，或者告知、取得同意将妨碍国家机关履行法定职责的除外”。据此，“告知+同意”仍旧是公权机关处理个人信息的首要法则，其对公权机关的适用与私主体在原则上并无不同。又根据《个人信息保护法（草案）》的说明，强调“知情同意”对于国家机关的适用，其目的也在于提高国家机关在处理个人信息上的透明度，凸显个人在数据处理中的自主地位。但国家机关在履职中对此原则的适用存有明确的例外，包括“法律、行政法规规定应当保密”以及“告知、取得同意将妨碍国家机关履行法定职责的除外”等情形。从这个意义上说，《个人信息保护法（草案）》虽然在规范构造上将同意同样作为公权机关处理个人信息的法则，但在适用效果上，却如欧盟GDPR一样，削弱了知情同意原则对于公权机关履职行为的约束。

但《个人信息保护法（草案）》第35条的规定也引出如下问题，是否所有的执法信息都要在“知情同意”原则下豁免，是否公权机关进行的所有公职行为都无须再接受“知情同意”的检验，而仅依赖部门职权或是法律授权即可获得合法性基础。此外，在考虑知情同意原则的公法适用时，除了要对从知情同意中豁免的“执法信息”的边界范围进一步廓清外，私法领域中有关改变传统“强同意”构造，“在明示同意之外增加拟制同意，以综合的情境合理判断替代单一的告知前提，从而缩减信息自决空间、降低同意生效标准、增强适用灵活性”[55]等，用以解决这一原则适用所引发的数据保护和数据利用矛盾的思路，同样也应被吸纳于公法保护的制度构建中。

（四）比例原则与数据最小化

个人信息并非为个人所独占，在个人数据之上同时承载了个人利益、社会利益和公共利益；对个人信息的保护，也不能放弃数据流通的目的，而两者的平衡又须在对个人利益、他人利益、企业利益、市场利益和公共利益全面权衡的基础上实现。很多时候，为了满足公共利益的保护需求，个人都须让渡其部分乃至全部的信息权利。但依据基本权利教义，基于公共利益而对个人权利的克减又必须遵守限度、合乎比例，否则就会造成对此种权利的彻底否定和排除。

〔55〕 蔡星月：《数据主题的弱同意及其规范结构》，载《比较法研究》2019年第4期，第80页。

相比美国是采取个案权衡和“场景理论”〔56〕就公共利益对个人信息权的限制边界进行具体化判定，欧盟主要采用比例原则来处理个人数据权与公共利益之间的冲突。欧盟 GDPR 第 5 条规定的“个人数据应：（c）充分、相关及以个人数据处理目的之必要为限度进行处理”正是比例原则。这一原则在数据法领域又常被总结为“数据最小化”原则，也同样被纳入我国《民法典》中。〔57〕除《民法典》外，《个人信息保护法（草案）》中同样对比例原则和数据最小化予以具体规定，其第 20 条规定，“个人信息的保存期限应当为实现处理目的所必要的最短时间”，体现的也是比例原则的要求。而在《个人信息保护法（草案）》“国家机关处理个人信息的特别规定”一节中，比例原则对国家机关同样适用且被特别强调。〔58〕

比例原则和数据最小化首先强调的是在数据收集方面的“有限原则”，即“无必要不收集”；其次还旨在防堵数据控制者对于所收集数据的深度分析和过度适用。本质上，比例原则和前文所说的数据战略中所倡导的“数尽其用”之间存在根本性矛盾。就数据库本身而言，其天然具有自我膨胀的本能，而且数据信息和数据资料越详尽越全面，其价值也会越高。因为数据与个人之间的匹配度越高，其所包裹的利益就越大。因此，无论是作为数据控制者的公权机关还是私主体，都会存在过度收集和深度分析数据的趋向。在私法领域，对数据的过度收集和深度分析，会导致个人因数据人格被贬损而彻底客体化；在公法领域，如果对于政府收集和分析数据的行为不加限度限制，也很容易就引发政府通过对数据的广泛采集和深度分析，而对人群进行“数据监控”。这种数据监控不仅会造成公民生活的透明化，会屏蔽异见和反对声音，也会诱使政府根据数据对人群进行“数据歧视”和“数据操控”。〔59〕此外，数据的大量聚集，亦会为数据安全带来隐患，这些因素都成为比例原则发生作用的原因。

比例原则和数据最小化原则虽然在约束公权机关无限度收集个人信息方面至关重要，但在实践中很容易被突破。例如 2011 年修订的《计算机信息网络国际联网安全保护管理办法》第 8 条规定，“从事国际联网业务的单位和个人应当接受公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为”。实践中，部分公安机关要求企业提供用户的详细注册信息和登录日志信息的事件频频爆出。因此，究竟何种信息属于“履行法定职责所必需的范围和限度”，比例原则在数据权的公法保护中又如何具体展开仍需要进一步细化。

〔56〕“场景理论”为海伦·尼森鲍姆所提出，这一理论的核心是批判脱离场景与信息关系谈论个人信息权利保护，而是在不同场景和信息关系下，通过分别分析场景、行为者、信息种类、传输原则等要素来得出不同场景下个人信息保护的不同边界和不同规则。Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009, p. 140 – 160.

〔57〕 参见《民法典》第 1035 条。

〔58〕 参见《个人信息保护法（草案）》第 34 条。

〔59〕 在中国“基因歧视第一案”的“三考生诉佛山市人保局案”中，被告佛山市人保局在招考公务员时进行基因检测，并基于基因检测结果作出相关决定。考生认为该行为超出了公务员招考的必要程序而诉至法院，但法院却最终以人保局并未将检测结果向外公布或泄露而判决不支持原告的诉讼请求。参见郭瑜：《个人数据保护法研究》，北京大学出版社 2012 年版，第 178 页。

## 四、“用户—平台—国家”三边关系下的国家积极义务

国家在数据保护中所承担的消极义务在于防堵国家对于个人信息的无限度收集和不当使用。但除国家公权机关外，个人作为信息主体的信息保护和数据安全还同时面临其他私人主体的威胁。在数据时代，信息主体与信息控制者之间的矛盾又主要呈现于“用户—平台”的私法关系中。

互联网平台迄今已逐渐蜕变为市场经济和社会生活的全新资源配置与组织方式。平台化使现实世界中的亲缘、地缘关系几乎都转化为平台关系，用户和平台也不复传统经济模式下的消费者与生产者。二者虽然都参与平台，但用户是平台数据的生产者，客户则为数据买单；而平台又通过将“用户”与“客户”予以连接，从而产生出一种可持续的盈利模式。在此，“算法成为统合平台的逻辑，数据成为平台发展的基础，而用户则被彻底降格为数据”。〔60〕平台的盈利基础在于用户所提供的信息，用户在产出这些信息时又几乎并未耗费任何成本。但当海量信息汇集于平台时，数据安全和信息保护问题就会凸显。

### （一）国家介入的必要

在此前相当长的一段时间，我国都是从信息安全的角度处理上述问题，此种信息安全又主要集中于计算机系统安全或运行安全。〔61〕信息安全观念所导出的信息保护，也由此主要依赖于“权限管理、病毒查杀、设立防火墙、VPN、入侵检测”等技术路径，其主要突出计算机的“运行安全和系统安全”，而并未包含对个人信息权的保护。因为主要依赖技术处理，法律的作用也在很大程度上被排除。在《民法典》纳入对个人信息的保护，且《个人信息保护法（草案）》也明确将个人信息予以权利化处理后，上述信息安全的传统观念也被渐次放弃。对用户信息的保护不仅是公共政策的要求，也是权利保护以及法律适用的结果。但如上文所述，因为数据技术上的云泥之别，用户和平台之间的关系不能仅依赖私法调整，此时必须强调国家介入，而这也成为国家在个人信息保护中所应负担的积极义务。

国家对信息主体和数据控制者私法关系的介入，同样可在欧盟 GDPR 中找到依据。欧盟曾在 95 指令中倡导各成员国确立一个或多个公共机构，负责个人数据保护的执行，这些机构不仅独立行使职权，而且被配备以调查权、有效干预权和参与诉讼的权利。95 指令的倡导后来被吸收入 GDPR 中。除吸纳这种模式外，GDPR 还对数据保护官的地位、职能进行了相当充分的规定。数据保护官制度被认为是欧盟“信息公法保护”模式的典型表现。与这种制度相连，GDPR 对于私人的数据处理还规定了相应的申报制度，即数据控制者及其代表在“实施任何意图满足某一目的

〔60〕“用户是数据”本质上是一种中性化的表达，并不涉及价值判断，原因是数据是事物在互联网时代的基本存在形式，唯有将一切降格为数据，事物之间的连接才会成为可能。参见［美］尼古拉·尼葛洛庞蒂：《数字化生存》，海南出版社 1999 年版，第 58 页。

〔61〕例如 1994 年制定的《计算机信息系统安全保护条例》的目的就在于保护计算机系统的安全，保障计算机及其相关功能的正常发挥，网络运行环境的安全；2004 年由公安部、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的《关于信息安全等级保护工作的实施意见》（公通字〔2004〕66 号）也侧重于信息安全等级的建立。

或是若干相关目的的全部，或部分自动化数据处理操作或成套此类操作前，都须向本国的数据保护机构申报”。以“数据官”和“数据申报制度”为代表的公法保护模式曾遭诸多民法学者反对，被认为“加重了个人数据处理者的负担”，也“反映除依赖管理的国家主义视角……”〔62〕，但迄今却被认为为“完善信息控制者内部治理机制”，“构建数据合作治理”〔63〕奠定了基础，且为诸多国家效仿。

事实上，要求国家介入的原因除了在于信息主体与数据处理者之间的不对等地位外，还在于数据控制者本质上并无动力去保护个人数据，因为数据滥用直接的受害者只是信息主体，而并非数据控制者。而且在网络环境下，因为数据的“随时产生、多点存储、多次开发、跨场景应用、多人经手、跨国境传输、收集与处理分离、生命周期短”〔64〕等原因，数据控制者若对个人数据加以高密度保护，不仅在技术上有很大难度，也会产生较高成本，这些因素都决定了其不可能自发地保护个人信息，外部监管和国家介入也因此变得必要。〔65〕

因为欧盟 GDPR 的影响，此次的《个人信息保护法（草案）》明确确立了公共数据机构对于私人主体数据收集和处理行为的监管模式。依据该法第 56 条，在我国负责履行个人信息保护职责的主要部门为国家网信部门，此外“国务院有关部门”，主要包括工业和信息化部、公安部、中国人民银行等，在各自职权范围内负责个人信息的保护和管理工作。这一规定在相对集中的个人信息监管体系基础上，兼顾了各部门和各行业的差异。但本条并未涉及国家网信部门和国务院相关部门的监管职责划分。此外，上述规定仅涉及中央层面，《个人信息保护法（草案）》在地方层面仅明确了县级以上地方人民政府有关部门履行个人信息保护和监督管理职责。由此，在未来的数据实践中，如何廓清各部门之间的职责界限，如何塑建涵括中央和地方的信息监管体制，仍有待探索。

（二）国家如何介入？

传统上，国家对私法关系的介入主要通过责任追究（包括刑事责任和行政责任）来进行，这种方式同样被应用于数据保护领域。从域外经验来看，信息保护法的一项重要目的在于通过构建有效的外部执法机制，借由制裁威胁和责任追究来敦促信息控制者履行个人信息保护的法律责任。事实上，即使如美国这样在信息保护中强调“行业自律”的国家，也会借助强大的外部执法机制来约束信息控制者的行为。〔66〕而欧盟 GDPR 也针对 95 指令缺乏有效的执法威慑和责任追究的问

〔62〕［德］克里斯托弗·库勒：《欧盟的隐私与数据保护》，温珍奎译，载周汉华主编：《个人信息保护前言问题研究》，法律出版社 2006 年版，第 46 页。

〔63〕 周汉华：《探索激励相容的个人数据治理之道》，载《法学研究》2018 年第 2 期，第 11 页。

〔64〕 周汉华：《探索激励相容的个人数据治理之道》，载《法学研究》2018 年第 2 期，第 6 页。

〔65〕 主张信息保护依赖于“行业自律”的观点来自美国法的启发，美国在信息保护领域注重“轻管制”，对于那些未被单项信息保护立法涉及的行业组织，一般采取行业自律的方式，即通过自我约束来达到对个人信息的保护，其理由是如果过度限制数据传播，将会抑制经济活动。郭瑜：《个人数据保护法研究》，北京大学出版社 2012 年版，第 53 页。

〔66〕 美国联邦贸易委员会、各州总检察长、民事诉讼、国会监督与媒体监督及社会监督等机制并不亚于欧盟国家个人信息管理局的执法力度。对于一些特殊的个人信息，例如征信信息、未成年人信息、金融信息、健康信息、电子通讯等，还有专门的联邦立法及相应的执法机构，保护力度也更大。周汉华：《探索激励相容的个人数据治理之道》，载《法学研究》2018 年第 2 期，第 17 页。

题，通过确立牵头数据管理局，加强各国执法合作，提高罚款幅度，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，大大强化了外部威慑机制。[67]

我国此前对信息控制者的责任追究方式主要在于2015年《中华人民共和国刑法修正案（九）》中所规定的“侵犯个人信息罪”和“拒不履行信息网络安全义务罪”，行政处罚则在后来规定于《网络安全法》第59条至第75条的“法律责任”一章中。但从实践效果来看，上述责任规定却存在过于倚重刑事制裁、刑事制裁与行政处罚无法有效衔接、行政处罚部分责任规范与行为规范相互脱节等问题。[68] 即使是看似严苛和宽泛的刑事制裁，因为带有象征性立法的顽疾，实际作用效果也相当有限。[69]《民法典》也仅仅是搭建了信息保护的基本制度框架，并未包含责任承担和追究的体系安排。因此，就需要专门的《个人信息保护法》在综合治理的框架内，通过纳入责任要求、明确行为规范、完善行政责任和刑事责任的有效衔接、加大违法成本、提高违法行为被发现的可能性等方式，构筑有效的责任追究和执法威慑的外部机制。

从目前提交审议的《个人信息保护法（草案）》来看，国家对于平台的监管同样遵循了“常规执法+责任追究”的模式。从常规执法来看，因为草案明确了国家网信部门对于信息保护的统筹协调和监管职能，因此，信息监管手段也被作为其“履行个人信息保护职责”的基本举措而予以规定，具体样态包括“……（一）询问有关当事人，调查与个人信息处理活动有关的情况；（二）查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料；（三）实施现场检查，对涉嫌违法个人信息处理活动进行调查；（四）检查与个人信息处理活动有关的设备、物品；对有证据证明是违法个人信息处理活动的设备、物品，可以查封或者扣押”。[70] 此外，《个人信息保护法（草案）》第60条延续了《网络安全法》的一般做法，在信息监管中纳入了约谈制度。“约谈”一直以来被作为一种软性的行政方式，它具有一定的威慑性，但同时也侧重于行政部门与相对人的沟通协调，将其运用于个人信息处理的风险防御与安全控制，有助于促成信息管理的合作治理格局。与《网络安全法》不同的是，《个人信息保护法（草案）》所规定的约谈事项已经不限于“网络存在较大安全风险或者发生安全事件的”，而是扩张至“个人信息处理活动存在较大风险或者发生个人信息安全事件的”。从责任规定来看，《个人信息保护法（草案）》第62条显然是汲取了欧盟GDPR的监管思路，相较《网络安全法》大幅提高了处罚幅度，还规定违反信息保护法的行为需同时适用信用联合惩戒。这些责任规定在很大程度上提高了个人信息的违法成本，由此将信息保护的外部压力通过严厉的制裁威慑而传导至信息控制者内部。

对欧盟GDPR的经验吸收还包括对行业自律和行业治理的强调，这一点与严厉的违法制裁一起构成了国家多元的介入方法。强调行业自律是为了弥补此前政府在平台治理中暴露出的局促与

〔67〕 周汉华：《探索激励相容的个人数据治理之道》，载《法学研究》2018年第2期，第12页。

〔68〕 周汉华：《探索激励相容的个人数据治理之道》，载《法学研究》2018年第2期，第14页。

〔69〕 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》，载《政治与法律》2017年第3期，第43页。

〔70〕《个人信息保护法（草案）》第59条第1款。

不足。因为在技术处理中的巨大优势，平台除了存在僭越个人信息、过度操纵市场的问题外，还一再构成对政府市场治理能力的削减。[71] 因为数据资源与处理能力的差异，政府已无力再通过传统的治理机制，作用于平台市场以大数据为基础的算法型运作过程，由此便产生这一领域的治理失灵或监管真空，这就使激励型的行业自治成为平台治理的重要途径。

在此思路下，《个人信息保护法（草案）》第五章专门加入“个人信息处理者的义务”，作为第四章“个人在个人信息处理活动中的权利”的对应。在第五章中，草案不仅详尽列举了个人信息处理者所应采取的必要措施[72]，还存在对事前的风险评估和信息泄露后报告义务的规定。前者强调个人信息处理者在进行个人信息处理活动前应对“个人信息的处理目的、处理方式等是否合法、正当、必要；对个人的影响及风险程度；所采取的安全保护措施是否合法、有效并与风险程度相适应”等问题进行评估；后者则要求个人信息处理者在发现个人信息泄露时，除立即采取补救措施外，还须及时通知履行个人信息保护职责的部门和个人。[73] 在外部的责任追究基础上，再辅以企业内部的自律治理机制，其目的都是促成《个人信息保护法（草案）》第 11 条所申明的“推动形成政府、企业、相关行业组织、社会公众共同参与个人信息保护的良好环境”，由此构建一种“权利控制与激励机制并行的多元治理机制”。[74]

## 五、结语

综上，《民法典》除将个人信息保护提升至全新高度外，更在私权保障基础上，纳入了对个人信息权的公法保护。但因为《民法典》并未对个人信息予以权利化处理，也未对个人信息的公私法保护如何展开进行细致规定，因此，在《民法典》时代如何构建和完善个人信息权的公法保护，就有赖于未来《个人信息保护法》的出台。

从目前已公布的《个人信息保护法（草案）》来看，其已着眼于建构一种包括公私在内的合作治理机制，而且在公法保护领域，有关国家消极义务和积极义务的框架结构也初现端倪。这一框架符合信息权作为个人基本权利的定位，也有助于我们对繁杂的数据保护问题予以体系化把握。借助这一框架，可对个人信息公法保护所涉及的核心问题予以定位，再通过对《个人信息保护法》的规范阐释和数据法的原理分析，对其内容进行明晰和填充，并在此基础上渐次完成我国个人信息公法保护的整体制度构建。

〔71〕 张兆曙、段君：《网络平台的治理困境与数据使用权创新：走向基于网络公民权的数据权益共享机制》，载《浙江学刊》2020 年第 6 期，第 38－42 页。

〔72〕 参见《个人信息保护法（草案）》第 51 条、第 52 条。

〔73〕 参见《个人信息保护法（草案）》第 54 条、第 55 条。

〔74〕 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》，载《法学研究》2018 年第 2 期，第 19 页。

# State Protection Obligation of Personal Information Right in the Era of Civil Code

ZHAO Hong

**Abstract:** Although the Civil Code does not treat personal information as rights, it has been incorporated into the protection of public law in addition to the protection of private law, thus promoting the protection of personal information to a new height. The public law protection framework of personal information can be divided into two aspects: the negative obligation and the positive obligation of the state. The former is to prevent the unlimited collection and improper use of personal information by the state, while the latter reveals the intervention and protection obligations of the state when facing the information controller whose status is not equal. The above-mentioned dual obligation framework has already appeared in the draft of the personal information protection law. On the basis of absorbing the experience of EU, the Personal Information Protection Law (Draft) has widely incorporated the responsibilities of public authorities in information protection. However, the provisions of the draft are relatively rough. Under the framework of the above-mentioned dual obligations, how to carry out the public law Protection of personal information still needs to rely on The principle of data law and the legislation and practice of foreign data are discussed in detail.

**Keywords:** Right to Personal Information; Public Law Protection of Personal Information; Negative Obligations of the State; Positive Obligations of the State

（责任编辑：傅广宇　汪友年）