财经法学 No. 2，2023
pp. 51 - 67

数字政府建设中个人信息保护的风险规制路径

刘绍宇*

内容提要：公共部门个人信息保护制度的完善是建构数字法治政府的必由之路。我国《个人信息保护法》采取了公私部门一体调整的宣示性立法模式，目前既无法为公共部门个人信息保护提供足够的规则指引，也未充分满足数字政府建设的需要。数字政府个人信息保护规则的建构，不仅需要考虑公共部门相对私人部门在个人信息处理活动中的特殊性，还要兼顾数字政府在技术和治理这两个层面的革新，进而制定专门规则。风险规制模式不仅是世界范围内个人信息保护制度的发展趋势，而且能够为一体调整模式提供理论基础。通过风险预防原则的适当运用，对个人信息权利的风险化解释与调适，风险管理、风险交流和风险评价等风险规制机制的灵活运用，以及合作治理、独立规制机构、技术治理、回应治理、试验规制和软法之治等风险规制策略的共同配合，建构以风险规制为导向的数字政府个人信息保护机制是我国未来的最优选择。

关键词：数字政府　个人信息保护　风险规制

一、问题的提出

近年来，我国一直致力于推动数字政府建设，并取得了令人瞩目的成绩。在数字政府建设中，政府汇集了整个社会的数据资源，并利用其实现大数据治理，这在提升行政服务水平、促进数字经济发展和推动国家治理现代化的同时，也带来了极大的数据安全和个人信息风险。数据全和个人信息保护是数字政府建设中不可忽视的议题，一直受到我国政府的高度重视。党的十九届四中全会作出的《中共中央关于坚持和完善中国特色社会主义制度 推进国家治理体

* 刘绍宇，中国社会科学院法学研究所助理研究员。

本文为国家社会科学基金重大项目“行政诉讼类型制度的构建研究”（19ZDA163）、中国博士后科学基金第 14 批特别资助“论私法主体的公法管控：以网络平台为考察对象”（2021T140727）阶段性研究成果。

系和治理能力现代化若干重大问题的决定》明确提出“推进数字政府建设，加强数据有序共享，依法保护个人信息”。而在 2022 年 6 月 23 日发布的《国务院关于加强数字政府建设的指导意见》中，国务院更是以专章规定“构建数字政府全方位安全保障体系”，其中包括“加大对涉及国家秘密、工作秘密、商业秘密、个人隐私和个人信息等数据的保护力度”。

与此同时，我国个人信息保护法律体系建设也正稳步推进。尤其是 2021 年《中华人民共和国数据安全法》（以下简称《数据安全法》）和《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）这两部法律的颁行，标志着我国个人信息保护法律制度基本成型。然而，尽管个人信息保护对数字政府建设来说至关重要，但个人信息保护制度的建构似乎与数字政府建设平行进行，并未为后者提供足够的制度供给。《个人信息保护法》采取公共部门与私人部门一体调整模式，被认为是一种“象征性立法”〔1〕，远远无法满足数字法治政府建设的制度需求，“数字政府建设过程中的个人信息保护尚未得到应有的重视”〔2〕。一体调整模式既无法为公共部门个人信息保护提供足够明晰的规则指引，也未回应数字政府建设的需要，“个人数据权利保护的制度供给不足是当前掣肘数字政府变革的重要因素之一”〔3〕。

如何规范公共部门个人信息处理活动，尤其是如何建构与数字政府兼容的个人信息保护制度，是建设数字政府和完善个人信息保护制度的重大议题之一。尽管目前学界已对政府处理个人信息活动的规范展开了深入研究，〔4〕但绝大多数研究并未充分考虑政府数字化转型的时代背景，而仍是在传统政府视角下的探讨。事实上，学界普遍认为数字政府给个人信息保护制度带来了极大的挑战，有学者直接指出数字政府与个人信息保护之间存在难以弥合的矛盾，〔5〕还有学者考察了开放政府、数据治理、平台政府与个人信息保护之间的冲突，〔6〕以及知情同意原则、目的限制原则与数字政府之间的张力〔7〕。

对于如何建构数字政府个人信息保护制度这一问题，学界存在权利保护路径和风险管理路径之间的争议。权利保护路径侧重于探讨个人信息保护原则以及个人信息权利如何在数字政府中实现，风险管理路径则认为应通过政府内部风险管理实现个人信息保护。本文认为应整合上述两种

---

〔1〕 王锡锌：《行政机关处理个人信息活动的合法性分析框架》，载《比较法研究》2022 年第 3 期，第 94 页。

〔2〕 马颜昕等：《数字政府：变革与法治》，中国人民大学出版社 2021 年版，第 370 页。

〔3〕 董筱文、胡雯：《以法治化赋能数字政府建设》，载《中国社会科学报》2022 年 8 月 10 日，第 8 版。

〔4〕 参见赵宏：《告知同意在政府履职行为中的适用与限制》，载《环球法律评论》2022 年第 2 期；喻文光、郑子璇：《数字时代政府机关处理个人信息告知义务制度的公法建构》，载《人权》2022 年第 3 期；彭錞：《论国家机关处理个人信息的合法性基础》，载《比较法研究》2022 年第 1 期；孙清白：《国家机关处理个人信息的特殊风险及其法律规制》，载《安徽大学学报（哲学社会科学版）》2022 第 3 期；程子栋、王鹏彪、罗海宁：《对数字政府安全技术合规分析的建议》，载《中国信息安全》2022 年第 8 期。

〔5〕 Vgl. Roßnagel/Laue, Zweckbindung im Elektronik Government, DÖV12 (2007), 543, 544; Hansen, Die ambivalente Beziehung zwischen eGovernment und Datenschutz, DuD 10 (2021), 664, 664; Stutz, Verantwortlichkeit und Datenchutz im E-government, in: Wind/Kröger (Hrsg.), Handbuch IT in der Verwaltung, 2006, S. 347.

〔6〕 参见宋烁：《论政府数据开放中个人信息保护的制度构建》，载《行政法学研究》2021 年第 6 期；宋华琳、郑琛：《论政府数据开放中的数据安全保护制度》，载《中国司法》2022 第 3 期；彭箫剑：《平台型政府及行政法律关系初论》，载《兰州学刊》2020 年第 7 期。

〔7〕 参见马颜昕、吴敏慧：《数字政府建设中〈个人信息保护法〉适用的挑战与展望》，载《网络信息法学研究》第 11 期，中国社会科学出版社 2022 年版，第 122 页。

路径的优劣，提出一种风险规制路径，为建构数字政府中的个人信息保护提供理论基础和制度指引。本文第一部分从权力、技术和组织这三个层面系统讨论数字政府建设如何对个人信息保护制度构成挑战，在此基础之上，第二部分提出个人信息保护的风险规制路径，并对其在数字政府中的运用予以证成，最后探讨如何在风险规制路径下完善数字政府个人信息保护制度。

二、数字政府建设对个人信息保护制度带来的挑战

学界普遍认为我国个人信息保护制度与数字政府建设之间存在难以弥合的矛盾，数字政府建设给个人信息保护制度带来严峻挑战。这主要是因为，在目前的一体调整模式下，我国以私人部门为范式建构的个人信息保护规则并未考虑到公共部门的独特之处和数字政府的最新发展。本文结合数字政府的主要特征，从公共属性、技术进步和治理革新这三个层面分析数字政府建设何以为个人信息保护制度带来挑战。

（一）公共属性给个人信息保护制度带来的挑战

我国《个人信息保护法》确立的一体调整模式，本质上是将以私人部门为范式建构的个人信息保护规则适用于公共部门，并未顾及数字政府的公共属性。公共属性是政府的固有属性，意味着政府主要是为了完成取向于公共福祉和公共利益的公共任务，进而被法律赋予职权。政府的公共属性并不因为其数字化转型而丧失，而应予以特别保护。公共部门之所以要有专门的个人信息保护规则，主要是基于其公共属性，这也是一体调整模式制度供给不足的首要原因。正基于此，在个人信息保护立法较为悠久的德国，公共部门个人信息保护立法一直独立于私人部门存在。

公共部门之所以给以私人部门为范式建构的个人信息保护制度带来挑战，主要是基于两个方面的原因。一方面，政府完成公共任务主要是为了维护公共利益，而个人信息保护制度主要是一种维护个人权益的机制。政府在履行公共职责时，个人信息保护原则和个人信息权利均会因为公共利益的优位性而受到限制。欧盟《保护警察和刑事司法当局使用的个人数据指令》（以下简称LED）和德国各州公共机构数据保护立法之中均对知情同意原则、目的限制原则和透明原则有不同程度的放宽，对个人信息权利也有一定限制。〔8〕甚至有学者认为目的限制原则被完全突破，因为与欧盟《通用数据保护条例》（GDPR）不同的是，只要符合合法性和必要性原则的要求，个人信息被再次处理的目的并不需要与初始目的兼容。〔9〕另一方面，政府无论是从事秩序行政还是服务行政，个人信息主体均处于一种非对等关系的弱势地位，诸如“同意”这样的个人信息保护机制基本失灵。有德国学者以疫情防控软件为例，指出该情境下政府搜集个人信息获取的同意根本无法实现有效的权利保护。〔10〕

---

〔8〕 See Mark Leiser & Bart Custers, The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680, 5 (5) *European Data Protection Law Review* 367, 373 (2019).

〔9〕 See Catherine Jasserand, Law Enforcement Access to Personal Data Originally Collected by Private Parties: Missing Data Subjects' Safeguards in Directive 2016/680?, 34 (1) *Computer Law & Security Review* 154, 163 (2018).

〔10〕 Vgl. Samardzic/Becker, Die Grenzen des Datenschutzes: Der beschrankte Schutz durch Freiwilligkeit und Einwilligung bei Corona-Apps, EuZW 31 (2020), 646, 646.

根据政府活动公共属性的高权程度不同，个人信息保护规则也应有所不同，而我国目前的一体调整模式并未作出这种区分。以欧盟为例，政府警察、刑事司法活动和一般行政活动的个人信息保护规则并不相同。一般来说，政府活动高权程度越高，相应的公共属性越强，对公民基本权利的影响越大，对以私人部门为范式建构的个人信息保护制度形成的挑战越大，特别规则的建立也越有必要。根据高权程度的不同，政府活动可以区分为警察和刑事司法活动、秩序行政、服务行政和私行政。结合前述原理，私行政活动可参照《个人信息保护法》其他部分的规定，因此“同意”在政府处理个人信息中也有适用空间。〔11〕警察和刑事司法活动高权属性最强，绝大多数国家建立了专门的个人信息保护规则。我国刑事诉讼法学界也对此展开了专门的深入研究，普遍认为应进行刑事诉讼个人信息保护专门立法。〔12〕一般秩序行政和服务行政则基本可以参照私部门个人信息保护规则，适用一体调整模式。不过，由于各个国家对警察、犯罪和刑事司法等概念的理解存在差异，警察、刑事司法活动和秩序行政实际上存在一定区分难度，在欧盟实践中已经造成困扰。〔13〕

（二）技术手段给个人信息保护制度带来的挑战

数字政府给个人信息保护制度带来挑战的另一关键原因在于，数字政府广泛运用了大数据、人工智能、区块链、云计算、物联网乃至虚拟现实和深度合成等新型数字技术。个人信息保护制度的本质是技术监管工具，〔14〕从监管理论上来说，其应随着技术进步而更新，否则会造成规制滞后。我国目前的个人信息保护制度整体上根植于 20 世纪 80 年代的公平信息实践，上述每一项技术革新均给其带来冲击，对此法律与技术界已展开了深入的探讨。〔15〕而数字政府是上述技术的综合运用，〔16〕更给个人信息保护带来系统性风险和根本性挑战。具体来说，数字技术的发展在以下几个方面给个人信息保护制度带来挑战，这些挑战目前已在数字政府建设中凸显。

1. 个人信息与非个人信息的区分

传统个人信息保护制度是建立在个人信息与非个人信息二分基础之上，个人信息被认为是个人信息保护立法的核心与前提。而在数字政府建设的大背景下，为了充分发挥大数据技术的治理潜力，数据融合越来越频繁，个人信息与非个人信息的区分开始模糊，非个人信息被重新识别的难度越来越低。早在《个人信息保护法》出台之前，关于个人信息的界定处于众说纷纭的状态，司法实践中也是莫衷一是。《个人信息保护法》出台后，尽管其对个人信息作出了较为明确的定义，但上述分歧并未完全消失。至今，个人信息的界定，仍然困扰着理论与实务界。在大数据时代，这一问题在未来根本无法得到解决，本质上是因为大数据技术使得重新识别越来

〔11〕 参见前引〔4〕，彭錞文。

〔12〕 参见裴炜、张桂贤：《论刑事诉讼中个人信息保护的知情规则》，载《成都理工大学学报（社会科学版）》2022 年第 4 期；郭烁、杨默涵：《受限、契合与独立：论刑事诉讼数据处理原则》，载《北京航空航天大学学报（社会科学版）》2022 年第 4 期；郑曦：《刑事诉讼个人信息保护论纲》，载《当代法学》2021 年第 2 期。

〔13〕 Vgl. Kugelmann, Anwendungsbereich und Spielraume der Landesdatenschutzgesetze, in: Seckelmann (Hrsg.), Digitalisierte Verwaltung Vernetztes E-government, 2. Aufl., 2019, S. 432.

〔14〕 Vgl. Vogel, Das Datenschutzrecht als Instrument der Technikregulierung, in: Susanne/Carsten/Brian (Hrsg.), Digitalisierung, Automatisierung, KI und Recht. Festgabe zum 10-jährigen Bestehen der Forschungsstelle RobotRecht, 2020, S. 645.

〔15〕 See Tal Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 (4) *The Seton Hall Law Review* 995 (2016).

〔16〕 国务院发布的《全国一体化政务大数据体系建设指南》中指出，积极运用云计算、区块链、人工智能等技术提升数据治理和服务能力。

越容易。

2. 目的限制原则

目的限制原则是我国个人信息保护制度的基础原则，规定在《个人信息保护法》第6条第1款中。所谓目的限制原则，是指个人信息的收集和利用均限于最初确立的目的，与该目的保持一致。从一定程度上说，目的限制原则和大数据技术的运作模式存在根本冲突。在数字政府的大背景下，大数据技术的要义便在于不断去发掘数据的价值，使数据发挥在搜集时难以预料到的作用。而目的限制原则要求个人信息的利用限于搜集时的目的，阻碍了新功能和新服务的研发，不利于数据利用价值的发挥。因此，在数字经济建设的大背景下，目的限制原则受到越来越多的批判，不少国家也通过引入兼容性使用标准、无法预料标准和尊重场景原则等来缓和目的限制原则的严格要求。〔17〕而我国则仍坚持了严格的目的限制原则，因而加剧了个人信息保护制度与数字政府建设，尤其是大数据治理之间的冲突。〔18〕

3. 知情同意原则

知情同意原则是世界范围内个人信息保护法的核心机制，在我国个人信息保护制度中也发挥关键作用。《网络安全法》一度将同意作为个人信息处理唯一的合法性基础，《个人信息保护法》尽管规定了更加多元化的合法性基础，但知情同意原则仍具有基础地位。然而，知情同意原则作为落实个人信息自决的机制，其前提在于个人信息主体具有独立自主决定的能力，对此《个人信息保护法》也专门规定，要求知情同意必须“由个人在充分知情的前提下自愿、明确作出”。而在数字政府背景下，数字技术的应用使得个人信息主体根本不可能满足这一前提条件，用户对其个人信息的控制是虚幻的。〔19〕由于个人根本无法理解隐私协议，也无法理解数字政府建设中的数字技术，以及其对个人信息所带来的风险，这种同意并不是建立在充分知情基础之上。

4. 个人信息权利

个人信息权利在不少数字技术中也难以实现，具有代表性的例子是人工智能、区块链和云计算技术。就人工智能来说，在机器学习中如何确保删除权和被遗忘权在国内外数据合规实践中已经成为一个难题，“数据删除的要求实际上已经游离在一种不可能的边缘”〔20〕，“完全删除数据是一项计算密集工作，既不经济实用也不环保”〔21〕。就区块链技术来说，删除权和被遗忘权〔22〕等个人信息权利的行使与区块链记录的完整性、防篡改性、可追溯性等原生特性存在悖论，在技术

〔17〕 参见朱荣荣：《个人信息保护“目的限制原则”的反思与重构——以〈个人信息保护法〉第6条为中心》，载《财经法学》2022年第1期。

〔18〕 参见刘权：《论个人信息处理的合法、正当、必要原则》，载《法学家》2021年第5期。

〔19〕 See Neil Richards & Woodrow Hartzog, The Pathologies of Digital Consent, 96 (6) *Washington University Law Review* 1461, 1473 (2018).

〔20〕 翟凯：《论人工智能领域被遗忘权的保护：困局与破壁》，载《法学论坛》2021年第5期，第142页。

〔21〕 Michèle Finck, The Limits of the GDPR in the Personalisation Context, in U. Kohl & J. Eisler eds., *Data-Driven Personalisation in Markets, Politics and Law*, Cambridge University Press, 2021, p. 100.

〔22〕 Vgl. Martini/Weinzierl, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 17 (2017), 1251, 1251.

上难以实现。〔23〕就云计算技术来说，删除权和可携带权等个人信息权利在云计算架构中难以实现。〔24〕

5. 个人信息保护责任

数字技术的发展不仅给个人信息权利带来挑战，而且给个人信息保护责任分配也造成威胁，这在区块链和云计算技术中尤为明显。个人信息风险管理以确定个人信息处理者为前提，进而课以个人信息处理者一系列义务责任。在区块链技术中，由于其去中心化的架构特征，中心化的个人信息处理者并不存在，如何认定个人信息处理者，至今仍是困扰理论界和实务界的难题，导致个人信息保护责任难以明确。〔25〕在云计算技术中，由于涉及各方均难以决定个人信息处理目的，个人信息处理者与个人信息受托人，以及欧盟法上的数据控制者与数据处理者之间的区分很难明晰，〔26〕进而影响了个人信息保护责任的分配。

（三）治理理念给个人信息保护制度带来的挑战

除了技术手段之外，数字政府所蕴含的治理理念也给传统个人信息保护制度带来极大的挑战。从传统政府到数字政府，本质上是为了“建设人民满意的服务型政府”，在治理理念上发生了整体政府、合作政府和平台政府的转变，传统个人信息保护制度无法满足变革所带来的制度需求。尽管数字技术在建构数字政府进程中发挥着举足轻重的作用，但治理理念的变革更为重要。理念是目的，技术只是工具，否则数字政府只会沦为一种形象工程。

首先，从政府内部关系来说，数字政府正在向整体政府转型。整体政府理念最早源自西方，核心在于整体性协作，其内容十分广泛，既包含不同层级政府之间的上下协作，也包含同一层级不同政府之间以及同一政府不同部门之间的左右协同，还包括政府与企业和非营利组织之间的内外合作。近年来，我国行政管理改革和法治政府建设也被认为发生了向整体政府的转变，〔27〕尤其是数字政府建设更是贯穿了整体政府的理念。在数字时代，数字技术的兴起和运用使得整体政府的理念更容易得到贯彻，整体政府进而也成为数字政府的重要特征。尤其是政府组织内部的数据共享打破了以往各个机构之间的信息孤岛，在线协作、跨部门协同和线上线下的交互融合协同，实现了整体性协同运行的路径建设。

其次，从政府企业关系来说，数字政府正在向合作政府转型。数字政府建设需要大量的技术支撑和资源投入，政府根本没有足够的能力单独完成，此时只能引入民间资本和企业力量才能满足技术、资金、人力等方面的需求。因此，公私合作成为我国乃至全球数字政府建设的普遍模式，对私人企业的依赖是以往任何公私合作形式所无法比拟的，数字政府也基本成了一种合作政府。无论是数据治理、数据共享还是数据开放，公私合作均发挥着重要作用。以数据治理为例，

〔23〕 参见陈爱飞：《解释论视域下的区块链个人信息删除权》，载《南京社会科学》2022 年第 6 期。

〔24〕 See Marina Škrinjar Vidović, EU Data Protection Reform: Challenges for Cloud Computing, 12 (1) *Croatian Yearbook of European Law & Policy* 171, 183 (2016).

〔25〕 参见前引〔22〕，Martini、Weinzierl 文，第 1257 页。

〔26〕 参见前引〔24〕，Marina Škrinjar Vidović文，第 176 页。

〔27〕 参见王太高：《我国整体政府思想的形成及其展开——以〈法治政府建设实施纲要（2021—2025 年）〉切入》，载《探索与争鸣》2022 年第 1 期。

不少政府的大数据决策监测技术系统均是由私人企业提供；以数据共享为例，目前全国范围内各地政府均采取了公共数据授权运营的模式，将公共数据授权给企业运营。

最后，从政府公民关系来说，数字政府正在向平台政府转型。平台政府的理念与实践发源于英国，近年来受到我国学界的高度关注。平台政府是我国数字政府建构的重要面向，搭建政务服务平台是近年来的主要工作。尽管国内外理论与实务界对平台政府的界定尚未达成共识，但整体上来说其具有如下两个方面的特征：组织技术上借鉴平台企业运用了双边平台治理技术和组织架构；治理理念上突出社会开放性、权力多中心、双向互动和公众参与。从外部关系来说，平台政府体现了开放、参与、便民和透明的价值导向；从内部关系来说，平台政府体现了协作、整体、效能和集成的管理理念。

数字政府具有显著的整体性、系统性、开放性和协同性特征，不仅将公共部门各个实体有机融合，而且将公共部门和私人部门高度整合。正基于此，越来越多的学者提出数字生态理论，认为数字政府、数字社会和数字公民构成了一个生态系统，充分体现了数字政府的治理转型。〔28〕随着数字经济的发展和数字政府建设的推进，这种特性会越来越强。而传统个人信息保护制度是建立在公私部门相互隔离和数据处理者分散独立的基础之上的以数据处理者为中心的调控模式，难以满足数字治理生态系统下的个人信息保护需求。基于此种范式，公共部门与私人部门之间的数据传输并未受到足够的规范，这在欧盟数据保护法中已经有所体现，〔29〕数据使用中的公私合作被认为处于法律真空状态，〔30〕在我国则更为明显；政府机构之间，政府机构与私人企业之间以及私人企业之间任何跨实体的数据流动被严格规范，个人信息一旦在不同的实体之间流动，便受到法律的管控；个人信息保护主要依赖于政府的行政监管和数据处理者自身的内部控制，个人信息主体参与性较低。

随着数字政府的不断发展，数字政府与传统政府在治理理念上的不同，已经演化为原则冲突甚至规则冲突。政府数字化转型所带来的治理理念变革被形塑为数字政府原则，甚至被进一步具体化为规则，例如，政府数据共享中的“以共享为原则、不共享为例外”正是整体政府的体现，一次搜集原则则同时体现了整体政府和平台政府的理念。但目前个人信息保护制度仍是基于传统政府而建构，严格的目的限制原则即是集中体现，即一旦个人信息被用于搜集时所确立目的之外的目的，均要得到授权。因此，有人提出一次搜集原则和目的限制原则存在冲突，〔31〕目的限制原则与整体政府之间存在冲突〔32〕。

---

〔28〕 参见孟天广：《数字治理生态：数字政府的理论迭代与模型演化》，载《政治学研究》2022年第5期；丁晓东：《从公开到服务：政府数据开放的法理反思与制度完善》，载《法商研究》2022年第2期；Groß/Krellmann，Das Okosystem der Digitalisierung，in：Stember/Eixelsberger/Spichiger/Neuroni/Habbel/・(Hrsg.)，Handbuch E-Government：Technikinduzierte Verwaltungsentwicklung，2019，S.7.

〔29〕 参见前引〔9〕，Catherine Jasserand文，第155页。

〔30〕 See Thilo Gottschalk，The Data-Laundromat? Public-Private-Partnerships and Publicly Available Data in the Area of Law Enforcement，6 (1) *European Data Protection Law Review* 21，21 (2020).

〔31〕 Vgl. Martini/Wenzel，„Once only“ versus „only once“：Das Prinzip einmaligerErfassung zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit，DVBL 132 (2017)，749，749.

〔32〕 参见前引〔7〕，马颜昕、吴敏慧文，第122页。

三、风险规制路径下的个人信息保护及其在数字政府中的应用

基于上述分析可发现，数字政府建设与传统个人信息保护制度之间存在内在矛盾，数字政府个人信息保护制度须进行体系性重构。本文提出一种风险规制路径来回应数字政府给个人信息保护制度带来的挑战，认为应以风险控制为导向，坚持适度预防原则，完善风险管理机制，并以风险规制理念重构传统个人信息保护规则。

（一）个人信息保护风险规制模式的提出及其与数字政府的契合

从全球范围来看，个人信息保护可以区分为“权利保护”和“风险管理”这两种模式，各国个人信息保护法均由这两种模式共同构成。权利保护模式起源于“公平信息实践”，随着个人信息保护在宪法层面的不断强化而被日益肯认，尤其是德国法上的信息自决理念和欧盟法上作为基本权利的个人信息保护观念的确立极大巩固了该模式。然而，该模式在如今互联网大数据时代受到越来越多的批判，其制度渊源（公平信息实践）和理论基础（信息自决）均受到各界的集体反思，不仅被认为无法满足时代发展的需求，〔33〕甚至还被批判有损于个人信息保护〔34〕。具体来说，一方面该模式依赖于个人信息主体对数据的控制，而这在互联网大数据时代由于数字技术的飞速发展、数据流动的日益频繁和平台权力的优势地位等因素根本无法真正实现；另一方面该模式使得人们陷入虚幻的安全，误以为对个人信息能够绝对控制，而忽视真正的风险。

在这一大背景下，各国数据保护法又开始了一场个人信息保护的风险革命，〔35〕风险管理的因素被越来越多地融入个人信息保护制度之中，进而形成了个人信息的风险管理模式。GDPR 正是这一观念转变的产物，其中大量规定了风险管理的内容，包括第 24 条规定的数据控制者基于风险的责任、第 25 条规定的通过设计的数据保护和默认的数据保护、第 35 条规定的数据保护影响评估。以上三种机制环环相扣、相互协调，构成了所谓的“风险三角”。〔36〕因此，GDPR 被认为发生了从权利保护法到市场监管法的转型。〔37〕

我国个人信息保护制度的建构过程尽管时间较短，但同样伴随着上述两种模式之间的争论。2016 年出台的《网络安全法》首次以法律形式系统规定个人信息保护制度时，便将知情同意原则作为唯一的个人信息处理合法性基础，充分体现了权利保护模式的理念。而在《中华人民共和国民法典》（以下简称《民法典》）编纂过程之中，在民法学界的大力推动下，个人信息更是被写入《民法典》人格权编，个人信息权有成为一项独立的人格权的趋势，权利保护模式得到进一

〔33〕 See Margot E. Kaminski, The Case for Data Privacy Rights (or, Please, a Little Optimism), 97 (5) *Notre Dame Law Review Reflection* 385 (2022).

〔34〕 See Ari Ezra Waldman, Privacy's Rights Trap, 117 *Northwestern University Law Review Online* 88 (2022).

〔35〕 See Claudia Quelle, The 'Risk Revolution' in EU Data Protection Law: We Can'T Have Our Cake and Eat It, Too, in R Leenes et al. eds., *Data Protection and Privacy: The Age of intelligent Machines*, Hart Publishing, 2017, p. 33.

〔36〕 See Claudia Quelle, Enhancing Compliance under the General Data Protection Regulation: the Risky Upshot of the Accountability-and Risk-based Approach, 9 (3) *European Journal of Risk Regulation* 502, 505 (2018).

〔37〕 Vgl. Schröder,„ Paradim Shift “ im Datenschutzrecht? -Wirtschaftsverwaltungsrechtliche Instrumente in der Datenschutz-Grundverordnung, in: Kronke (Hrsg.), Regulierung in Zeiten der Digitalwirtschaft: Ausgewahlte Fragen des Offentlichen Wirtschafts-, Informations-und Medienrechts, 2019, S. 13f.

步强化。而在《个人信息保护法》立法过程中，《民法典》所秉持的权利保护模式开始受到质疑，越来越多的学者提出风险控制的理念，〔38〕风险管理模式开始形成。至今，尽管《个人信息保护法》已经颁行，但这场争论尚未结束。〔39〕而从《个人信息保护法》的文本来看，立法者采取了折中路线，同时保留了这两种模式。

事实上，无论是权利保护模式还是风险管理模式，均存在利弊之处。尽管与权利保护模式相比，风险管理模式被认为是互联网大数据时代的更优选择，但其仍存在难以克服的不足。风险管理模式依托于元规制的规制理念，主要依赖于企业自身的内部控制，而由于风险概念的不确定性，很可能会导致个人信息保护的不均衡。由于企业占据主导地位，其在自身利益驱动下一旦缺乏刚性监管机制便很容易走向形式主义。对此，不少学者表达了深深的担忧，认为依靠企业自我规制的个人信息保护可能只是“口头上说说而已”，〔40〕甚至沦为一个走过场的纸质清单〔41〕。实践也证明了这种担忧，美国是风险管理模式的代表，尽管各互联网巨头均建立了表面看起来十分完善的风险管理体系，但是个人信息风险事件仍层出不穷。

有鉴于此，近年来越来越多的学者提出个人信息保护的风险规制模式。〔42〕该模式将权利保护和风险管理两种模式有机融合，将个人信息保护视为对数字技术的风险规制，认为个人信息保护制度的根本目的在于规制个人信息处理活动给公民权利、社会利益和国家安全等法益带来的风险。在风险规制模式中，个人信息权利并不被完全放弃，只不过不再被视为一种绝对权利，而是在风险理念下予以重构，被视为风险预防原则的体现和风险规制的工具。〔43〕国内外实务界在落实个人信息原则和保障个人信息权利时同样运用了基于风险的方法，间接证明了这点。不仅如此，通过设计和默认的数据保护，个人信息原则和权利被整合到企业内部风险管理之中，成为数据处理的一部分。在风险规制模式下，无论是权利保护还是风险管理，均服务于个人信息风险的预防，只不过侧重点有所不同：前者是以一种定型化的刚性方式，为个人信息保护划定最低限度的标准，后者则是以量体裁衣的灵活模式，由个人信息处理者根据具体情境自行把控，两者形成了一种相互配合刚柔并济的协作关系。〔44〕不仅如此，风险规制中的公共治理特征，与近年来个人信息保护理论中强调人与人之间关系的集体利益面向呼应。

---

〔38〕 参见丁晓东：《个人信息私法保护的困境与出路》，载《法学研究》2018 年第 6 期；吴伟光：《大数据技术下个人数据信息私权保护论批判》，载《政治与法律》2016 年第 7 期；周汉华：《个人信息保护的法律定位》，载《法商研究》2020 年第 3 期。

〔39〕 参见刘权：《个人信息保护的权利化分歧及其化解》，载《中国法律评论》2022 年第 6 期。

〔40〕 参见前引〔36〕，Claudia Quelle 文，第 524 页。

〔41〕 See Bert-Jaap Koops, The Trouble with European Data Protection Law, 4 (4) *International Data Privacy Law* 250, 255 (2014).

〔42〕 See Alessandro Spina, A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics, 8 (1) *European Journal of Risk Regulation* 88 (2017); Maximilian von Grafenstein, Refining the Concept of the Right to Data Protection in Article 8 ECFR-Part II: Controlling Risk through (Not to) Article 8 ECFR against Other Fundamental Rights, 7 (2) *European Data Protection Law Review* 190 (2021).

〔43〕 参见王锡锌：《重思个人信息权利束的保障机制：行政监管还是民事诉讼》，载《法学研究》2022 年第 5 期。

〔44〕 See Raphaël Gellert, We Have always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-based and the Risk-based Approaches to Data Protection, 2 (4) *European Data Protection Law Review* 481, 481 (2016).

本文认为，为了解决上文所述数字政府给个人信息保护带来的挑战，应以风险规制模式指导数字政府个人信息保护制度的建构。风险规制模式不仅是目前世界范围内个人信息保护的最优路径，而且能够为一体调整模式提供法理基础。近年来，世界范围内一体调整模式正在成为主流。在德国，尽管存在专门的公共部门数据保护规则，但是其和私人部门保护规则存在同构性。而在日本，分别立法模式也被转化为一体调整模式。这在风险规制模式下很容易理解，因为无论是私人部门还是公共部门的个人信息保护制度，其功能均在于规制数字技术带来的风险。风险规制模式不过分强调公共部门与私人部门之间的差异，而是侧重于在数字生态系统下数字风险本身的防范。正如德国联邦内政部在其发布的《数据保护法的现代化》报告中指出的那样，“一般数据保护原则同样适用于公共部门和非公共部门”，因为“在这两个领域必须保证同等的数据保护水平，这取决于风险而非领域”〔45〕。

（二）数字政府个人信息保护风险规制模式的建构

根据风险规制的理论与实践，风险规制是一种面向不确定性的规制，预防原则是其核心原则，风险管理、风险评价和风险交流是其主要内容，去中心化规制、试验规制、回应规制、技术规制、情境规制和独立规制机构是其规制特征，法律的不完整性与诸如标准等软法的突出地位是其表现形式。事实上，越来越多的研究和实践表明，目前个人信息保护法已经高度体现出了上述特征。考虑到数字政府本身的特点，本文就如何建构数字政府个人信息保护风险规制模式提出如下建议：

1. 数字政府个人信息保护风险预防原则的妥当运用

风险预防原则是要求决策者对不确定性引发的问题保持特殊注意的一项原则，〔46〕是风险规制的基本原则。近年来，越来越多的学者主张将风险预防原则引入个人信息保护制度之中。〔47〕其核心要义是于风险不确定之时即采取预防措施，这实际上早已在各国数据保护法之中充分体现。无论是传统个人信息保护原则，包括知情同意原则、目的限制原则、最小必要原则，还是新兴个人信息风险管理机制，例如个人信息保护影响评估，以及通过设计的个人信息保护，均是在风险尚未确定时即对数据处理活动进行限制，具有风险预防的功能。风险预防原则同样具有阻碍创新和限制产业的风险，因而也受到各界的诸多批评。在数字经济语境下，过于严苛的风险预防原则会阻碍数字技术的进步和数字经济的发展，如何平衡安全和创新之间的关系成为妥当运用风险预防原则的关键。德国学者将基于风险的路径与风险预防原则比较，在承认两者具有高度相似性的同时，指出前者由于风险评估等机制比后者更加精确。〔48〕风险预防原则被学界指责过于粗糙，因而也正在朝精细化的方向发展，例如苏宇提出在风险预防原则之中引入等级化或概率化的

〔45〕 Vgl. Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechtes-Gutachten im Auftrag des Bundesministeriums des Innern, 2001, Bundesministerium des Innern, S. 14.

〔46〕 参见赵鹏：《风险、不确定性与风险预防原则——一个行政法视角的考察》，载《行政法论丛》第 12 卷，法律出版社 2009 年版，第 105 页。

〔47〕 See Raphaël Gellert, Data Protection: a Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative, 5 (1) *International Data Privacy Law* 3 (2015); Joanna Mazur, Automated Decision-making and the Precautionary Principle in EU Law, 9 (4) *TalTech Journal of European Studies* 3 (2019).

〔48〕 Vgl. Appel/Mielke, Strategien Der Risikoregulierung: Bedeutung und Funktion eines Risk-Based Approach bei der Regulierung im Umweltrecht, 2014, S. 17 - 32.

合比例性要求，普遍建立反向证明机制及风险预防措施动态调整机制。如此精细化的风险预防原则和基于风险的路径殊途同归。〔49〕

具体来说，政府引入数字技术时应进行充分的风险评价和分析，在证明确实存在高度不确定风险时应适用严格的风险预防原则。近年来，人脸识别技术在国内外私人部门和公共部门都得到日益广泛的应用。作为一项新技术，人脸识别的风险具有高度的不确定性，其造成的损害一旦发生很可能难以挽回。对于这种存在巨大不确定性风险的新技术，政府有义务基于风险预防原则限制其使用。除此之外，对于大规模政务数据共享平台的建立，也应严格进行风险评价和分析，如果没有切实可行的数据安全与个人信息保护保障机制，集中化数据库会带来大量数据泄露风险，此时应考虑适用风险预防原则。〔50〕

2. 数字政府个人信息主体权利的风险化解释与调适

权利保护路径不应被完全放弃，其在目前仍具有不可替代的功能，但在大数据互联网经济的时代背景下应发生风险化转型，即以风险管理的理念对其予以解释和调适。这一做法不仅在理论上被不少学者所主张，在实践中也已经广泛运用。具体来说，在落实个人信息保护原则和保障个人信息权利时，应将它们视为风险规制的工具进而采取基于风险的方法，结合具体场景进行风险与收益的权衡，并通过法律、管理和技术的手段将其融入个人信息处理者风险管理之中。

对于数字政府语境下个人信息的判定，也应结合场景根据风险管理的方法展开。将匿名化的信息视为非个人信息是全球数据保护的通行做法，匿名化成为区分个人信息与非个人信息的关键。而如何认定匿名化在实践中遭遇了难题，这是因为其是一个具有较大弹性的相对概念，最终的判断只能是一项风险收益的权衡。〔51〕尽管匿名化措施能够在一定程度上降低个人信息风险，但绝对的匿名化在技术上不可能实现，且会损耗数据的使用价值，带来不菲的技术成本。如果数据进入公共领域，即便经过匿名化处理，其所面临的风险也更高。因此，在数字政府语境下，公共数据开放中的匿名化要求应比行政机关数据共享中更为严格。

就知情同意原则来说，同意机制在私人部门语境下尽管遭遇困境，但通过风险化转型仍能发挥重要作用。但是在数字政府语境下，其不仅面临互联网大数据时代的技术挑战，还受到公权力强制性和非对等性的侵蚀，进而基本丧失功能，甚至可能成为滥用数据权力的工具。不过本文认为，即便在数字政府语境下，同意机制也不应完全放弃，在服务行政领域仍有适用余地。此时同意机制构成了风险规制中的公众参与机制，即让公民自行决定是否承担个人信息风险。〔52〕知情权则仍发挥着风险交流作用，我国《个人信息保护法》也采取了保留知情权废除同意机制的做法。在数字政府语境下，知情权保障尤为重要，只有为了保障重要的法益才能被限制，且应符合法律保留和比例原则等法律原则的要求。

就目的限制原则来说，其尽管同样在互联网大数据时代由于阻碍数据治理和数字技术革新受

〔49〕 参见苏宇：《风险预防原则的结构化阐释》，载《法学研究》2021年第1期。

〔50〕 参见邢会强：《政务数据共享与个人信息保护》，载《行政法学研究》2023年第2期。

〔51〕 See Michèle Finck & Frank Pallas, They Who Must Not be Identified-distinguishing Personal from Non-personal Data under the GDPR, 10 (1) *International Data Privacy Law* 11, 11 (2020).

〔52〕 参见前引〔47〕，Raphaël Gellert文，第10页。

到越来越多的批判，但是对于对抗数据权力、降低个人信息风险和保障公民基本权利来说发挥着关键作用，〔53〕尤其在数字政府中没有同意机制的情况下其重要性更加凸显。不过，为了避免目的限制原则过于僵化，应对其予以风险化转型，即放弃传统权利保护理念下的严格立场，而转向风险管理路径下的场景分析。此时目的限制原则构成了一种风险预防机制，即在风险尚未成为现实危害之前提前采取预防措施。在数字政府语境下，目的限制原则的适用同样应结合具体场景展开风险收益权衡。例如在反恐等涉及大量公民生命权等重要法益的情况下，可以考虑适当突破目的限制原则的要求，但仍应严格遵循比例原则和法律保留原则的要求，并采取法律、管理和技术等方面措施尽可能将风险降低。除此之外，目的限制原则应融入政府个人信息合规管理流程之中，成为内部风险管理机制的组成部分。罗斯纳格尔（Roßnagel）教授专门指出，目的限制原则与数字政府之间的矛盾可以通过诸如内部权限管理这样的适法技术架构来克服。〔54〕

把目光投向个人信息权利，也可以得出类似的结论。个人信息权利并非实现个人对其数据控制的工具，而是风险规制手段。与知情同意一样，查阅复制权、删除权和解释说明权仍是实现风险交流和公众参与的方式，而更正补充权则是为了避免数据错误所带来的风险。在这种风险规制路径下，个人信息权利只能在风险规制之中发挥次要作用。为了真正规制风险，政府应起到首要作用，主动承担风险交流责任，推动公众参与，而不是被动地等待公民主张自身权利。实践表明，个人信息权利在公共部门所发挥的作用有限，公民向政府主张个人信息权利的积极性不高。在欧盟，有学者指出，为了实现更好的个人信息保护，较少关注个人信息主体的权利似乎有违直觉，但是从实际角度来看可能更为现实。〔55〕以解释权为例，政府应主动履行风险交流义务，向社会公众解释数据治理中算法的风险，解释权所能发挥的作用十分有限，〔56〕这种义务应成为政府个人信息合规管理的组成部分。

3. 数字政府个人信息保护风险管理制度的稳步建构

《个人信息保护法》出台后，我国企业纷纷开始建立个人信息保护合规管理体系。尤其是对于大型个人信息处理者来说，建立个人信息保护合规管理体系是实现数据合规的必备之举。因此，《个人信息保护法》在第 58 条第 1 项对超大互联网平台课以“建立健全个人信息保护合规制度体系”的义务。正如前文所指出的那样，数字政府具有整体性和协同性特征，属于大型个人信息处理者，参考《个人信息保护法》第 58 条的规定同样具有建立个人信息保护合规管理体系的义务。然而从目前来看，我国尚没有政府尝试建立个人信息保护合规管理体系，更多的是建立政务数据安全治理体系。尽管这两者之间存在共同之处，例如均属于风险管理活动，但是仍存在不少差异，前者主要围绕权利展开具有法律面向，而后者则围绕安全展开以技术面向为主。今后应努力在政务数据安全治理体系之中融入个人信息保护合规内容，着重从如下几点入手：

---

〔53〕 See Isabel Hahn, Purpose Limitation in the Time of Data Power: Is There a Way Forward?, 7 (1) *European Data Protection Law Review* 31, 31 (2021).

〔54〕 参见前引〔5〕，Roßnagel、Laue 文，第 549 页。

〔55〕 参见前引〔8〕，Mark Leiser、Bart Custers 文，第 378 页。

〔56〕 See Lilian Edwards & Michael Veale, Slave to the Algorithm? Why a ‘Right to an Explanation’ Is Probably Not the Remedy You Are Looking for, 16 (1) *Duke Law & Technology Review* 18, 18 (2017).

（1）完善数字政府个人信息保护合规管理。其一，设置专门个人信息保护负责人。《个人信息保护法》第52条规定，处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人。如果严格根据一体调整原则，绝大多数政府处理个人信息均能达到国家网信部门规定数量，应指定个人信息保护负责人。从目前我国各地数字政府情况来看，不少地方开始探索设置政府首席数据官，而其主要职能在于数据治理，并不具有个人信息保护职责。在欧盟法中，GDPR也要求公共部门设立数据保护官。2022年5月31日，法国国家信息保护委员会（CNIL）向法国22个城市发出通知，要求22个城市的地方政府必须在4个月内任命一名数据保护官（DPO），以符合GDPR的规定。在德国，设置数据保护官对于公共部门来说是一项强制性义务，而对于私人部门仅是一项自愿性义务。公共部门机构普遍设立了数据保护官，各州数据保护法均对数据保护官的任命、权限和职责问题进行了详细规定。这一模式未来也值得我国借鉴，未来可以考虑由政府首席数据官进一步承担个人信息保护职责，不过最优路径仍是设置专门的政府个人信息保护负责人。

其二，加强数字政府个人信息合规管理体系建设。私人部门丰富的个人信息合规管理实践经验为公共部门提供了参考，我国政务数据安全治理体系也基本包括了数据分级分类制度、内部管理制度和操作规范、安全技术使用规范、数据安全培训制度、安全审查和审计制度、第三方管理制度和突发事件应急管理制度。上述制度可以适用于个人信息保护，但并未充分考虑个人信息保护的特殊性。就目前来说，一方面应在政务数据安全治理体系之中融入个人信息合规管理，例如将个人信息纳入数据分级分类制度，在数据安全审计中纳入个人信息保护指标等；另一方面，还应结合个人信息保护特殊性建立一些专门的个人信息保护合规管理机制，例如个人信息保护投诉举报机制、个人信息权利响应机制、个人信息风险交流机制和个人信息跨境管理机制等。

其三，加强政府工作人员个人信息保护培训工作，建设公共部门个人信息保护合规文化，尤其应强化领导干部个人信息保护意识。个人信息保护工作高度依赖于人的观念、意识和知识，因此各国均高度重视个人信息保护培训工作和合规文化建设。就目前来说，我国针对政府首席数据官的培训工作在个别地方已经展开，但是个人信息保护并未成为重点授课内容。通过个人信息保护培训，能够强化政府工作人员的个人信息保护知识和技能，提升个人信息保护意识，进而在整个系统形成隐私和个人信息保护的文化。

（2）应建立政府个人信息风险评估机制。《个人信息保护法》第55条和第56条确立了个人信息保护影响评估制度，尽管该条文似乎是针对私人部门设计，但无论从法理还是域外实践来看，其应同样适用于公共部门。〔57〕随着数字政府建设的推进，大数据技术应用越来越广泛，政府个人信息处理活动的风险也与日俱增，不少风险存在不确定性，有必要予以评估。尽管我国政务数据安全治理体系之中已经包括数据安全风险评估，不少地方公共数据管理办法也规定了公共数据安全风险评估，但这并不意味着没有必要建立个人信息风险评估机制。前者仅能从技术角度对安全风险予以测评，而后者则是直接全面深入地对个人处理活动对公民权利、社会利益和国家

〔57〕 参见刘权：《论个人信息保护影响评估——以〈个人信息保护法〉第55、56条为中心》，载《上海交通大学学报（哲学社会科学版）》2022年第5期。

安全可能带来的风险进行分析。

（3）建立政府个人信息保护风险交流机制。风险交流是指风险信息的沟通，在风险规制中具有不可或缺的作用。〔58〕具体来说，是由政府机构主导，在专家和公众之间建立一定的交流平台，如互联网、媒体等，使专家和公众可以相互交换风险信息和观点，在帮助公众克服风险信息认知中的障碍和偏见的同时，也使公众对风险认知的一些价值判断成为风险规制机构作出风险决策的考量因素，从而弥补专家知识与公众认知之间的信息不对称。作为一种风险规制机制，个人信息保护也有必要引入风险交流机制。个人信息风险交流的不顺畅，也可能像环境领域那样引发激烈的、具有潜在破坏性的社会抗争活动。近年来，美国多个地区先后发生了大规模的反对人脸识别的游行示威，这是各地出台立法禁止人脸识别技术应用的重要原因之一，亚马逊、IBM、微软等公司都宣布终止了人脸识别产品的销售。

我国应从如下方面建构数字政府个人信息保护风险交流机制：首先，建立个人信息保护风险交流的责任机制。须明确的是，对于数字政府个人信息保护风险交流，政府应承担主体责任。而在政府内部，个人信息保护监管部门应成为风险交流的组织者，明确各方责任，为利益相关者的风险交流搭建平台。各地方政府和政府部门应由个人信息保护负责人作为风险交流执行者，向社会公众传递和提示个人信息保护风险，并向个人信息保护监管部门传递个人信息保护风险信息。其次，探索个人信息风险交流工具。要建立个人信息保护风险交流机制，还应努力探索合适的风险交流工具。从域外经验来看，风险信息交流主要是通过软法实现。在数字政府个人信息保护之中，也应充分发挥软法作用实现风险信息交流，例如制定《政府个人信息风险交流指南》。对于大规模搜集个人信息的公共服务应用，应向社会发布个人信息保护风险情况。最后，发挥专家在风险交流中的作用。作为“诚实的代理人”，专家既可为规制者服务，也可为被规制企业、利害关系方或一般公众服务。〔59〕

（4）加强个人信息保护风险规制中的公众参与。公众参与也是风险规制活动中的必备要素，其与风险交流存在密切关联，但也存在区别，两者容易混淆。风险交流侧重对风险信息的沟通，包括社会公众对风险信息的了解，而公众参与则在风险交流基础之上更进一步，强调社会公众参与风险规制决策。在数字政府建构中，有学者提出在政府中心主义路径之外借助数字技术的力量采取市民授权机制，〔60〕通过个人信息的公共信托和数据合作社等形式使利益相关者参与到数据治理体系之中，〔61〕这本质上是一种电子化的公众参与形式，在今后数字政府建设中可以探索采用。

4. 数字政府个人信息保护风险规制策略的灵活使用

从规制策略上来说，风险规制具有合作规制、独立规制机构、技术治理、回应治理、试验规制、软法之治和情境规制等诸多特征，这些规制策略对于数字政府个人信息保护建构来说也颇有

〔58〕 参见沈岿：《风险交流的软法构建》，载《清华法学》2015 年第 6 期。

〔59〕 参见金自宁：《风险规制中的信息沟通及其制度建构》，载《北京行政学院学报》2012 年第 5 期。

〔60〕 参见高翔：《超越政府中心主义：公共数据治理中的市民授权机制》，载《治理研究》2022 年第 2 期。

〔61〕 参见王锡锌：《数治与法治：数字行政的法治约束》，载《中国人民大学学报》2022 年第 6 期。

借鉴意义。

就合作规制来说，上述风险交流和公众参与，以及政务个人信息保护的政企合作均是合作规制的重要面向，即政府、企业和公民共同参与到政府个人信息保护的风险规制之中。除此之外，作为合作规制表现形式的公共部门的私人规制，〔62〕即通过私人规制公共部门的活动，在数字政府个人信息保护之中也应有所体现。例如可以鼓励多方主体参与推动数字政府个人信息保护国家标准、地方标准和团体标准等标准制定工作，考虑在法治政府评估指标体系中引入个人信息保护合规指标。

因为风险规制往往针对科技创新而开展，而科技一直处于高速发展之中，加上风险具有高度不确定性，所以回应规制和试验规制也构成了风险规制的惯常规制策略。〔63〕在数字政府建构中，诸多数字技术不断引入并更新迭代，这是个人信息风险的主要来源。为了应对数字技术所带来的不确定性风险，回应规制和试验规制的规制策略不可或缺。具体来说，应针对不断更新的数字技术及时通过试点和监管沙盒等形式探索与之匹配的规制机制。例如，近年来区块链和云计算技术在数字政府中的引入给个人信息保护带来挑战，应及时采取法律和技术的应对措施进行回应。欧盟在2022年计划系统解决公共部门云服务数据合规问题，尤其是云服务中的控制者和处理者关系与数据国际传输问题。

就软法之治来说，一直以来诸如标准这样的软法在风险规制领域扮演着尤为重要的角色。这在个人信息保护领域同样如此，有学者指出数据保护立法的非完全性，而这种非完全性在很多情况下正是通过标准的形式来补充。以我国《个人信息保护法》的实施为例，标准在个人信息保护合规实践中发挥着不亚于《个人信息保护法》本身的作用。目前，数字政府数据安全与个人信息保护的标准起草工作正在进行之中，尚没有专门政务领域的个人信息保护标准，现有标准中关于个人信息保护的内容也较少。从风险规制原理来说，个人信息保护法律制度供给的不足是一种合理状态，因为这更多需要软法来补足。公共部门个人信息保护制度的建构同样如此，未来应加强数字政府个人信息保护标准建设。不过值得注意的是，对于警察与刑事司法这样高权性较强的领域，应遵循严格的法律保留原则，禁止通过标准的形式规定个人信息保护规则。〔64〕

就技术治理来说，技术治理是风险规制的重要特征，通过设计的保护（Protection by Design）的理念最早兴起于化学监管和药品监管等风险规制领域。〔65〕在私人部门，通过设计的个人信息保护已经成为国内外数据保护的普遍实践，在实现数据合规中发挥着重要作用。对于公共部门个人信息保护来说，该理念也有重要的价值。除此之外，隐私计算通过数据的可用不可见对于目前公共部门和私人部门日益融合的数据治理生态具有巨大的潜力，〔66〕已经在私人部门和

〔62〕 参见〔英〕科林·斯科特：《规制、治理与法律：前沿问题研究》，安永康译，清华大学出版社2018年版，第91页。

〔63〕 参见董正爱、王璐璐：《迈向回应型环境风险法律规制的变革路径——环境治理多元规范体系的法治重构》，载《社会科学研究》2015年第4期。

〔64〕 Vgl. Marsch /Rademacher, Generalklauseln im Datenschutzrecht: Zur Rehabilitierung eines zentralen Bausteins des allgemeinen Informationsverwaltungsrechts, VERW 54 (2021), 1, 35.

〔65〕 See Mirella Miettinen, "By Design" and Risk Regulation: Insights from Nanotechnologies, 12 (4) *European Journal of Risk Regulation* 775, 775 (2021).

〔66〕 参见郑谐维：《隐私计算在政务数据共享中的应用》，载《上海信息化》2022年第4期。

公共部门得到了一定的应用，国务院办公厅印发的《全国一体化政务大数据体系建设指南》多次提及隐私计算技术。技术治理还能够通过技术方案实现更加有效的个人信息保护、风险交流和公众参与。例如私人部门的个人信息管理系统和同意管理工具均可运用于公共部门，公民可在其系统之中管理授权、查看个人信息访问情况和及时更正个人信息，进而能够更好地实现其个人信息权利和获知个人信息风险。

就独立规制机构来说，史蒂芬·布雷耶在论述风险规制体系时，首先提出的建议是建立独立规制机构。〔67〕建立独立规制机构可以说是风险规制的共同特征。作为一种风险规制活动，个人信息保护也有必要建立独立规制机构，这也是全球数据保护监管的一个趋势。〔68〕在域外实践中，数据保护监管机构不仅要负责监督私人企业，而且还要监督公共部门，进而形成政府内规制。〔69〕在欧盟，数据保护监管机构一直以来同样负责监督公共部门的个人信息保护，并在 LED 指令的意见中建议各个成员国成立专门数据保护监管机构，同时负责公共部门和私人部门的个人信息保护监督。欧盟数据保护机构（EDPS）在 2022 年初要求欧洲刑警组织删除与犯罪活动无关联的所有个人信息。日本 2021 年《个人信息保护法》修改过程中，赋予个人信息保护委员会（PPC）监督公共机构的权限。在我国，由于不存在个人信息保护独立监管机构，可以由《个人信息保护法》规定的履行个人信息保护职责的部门对各级政府个人信息保护合规状况进行监督。

四、结　论

对于数字政府个人信息保护制度的建构，学界存在权利保护模式和风险管理模式之间的分歧。本文认为上述两种模式各有利弊，无论何种模式均无法单独担负起个人信息保护的任务，因此提出风险规制模式作为数字政府个人信息保护的理论基础与实践指引。该模式有机整合了权利保护模式和风险管理模式，是个人信息保护制度的最优选择。更为重要的是，风险规制模式着眼于数字政府、数字社会和数字公民构成的数字生态中数字风险的一体化防范，同样适用于数字政府，进而构成了公共部门与私人部门一体调整模式的法理基础。正基于此，私人部门在数字化转型中积累的丰富风险规制经验可以运用到公共部门。

数字政府个人信息保护的风险规制模式，在行政法上还具有更加深远的启发意义。一直以来，传统行政法主要关注外部法律关系，即便是近年来行政法中兴起的规制理论也主要侧重于政府对市场主体的监管。这是因为，在物理世界中，私人部门是主要的风险来源。公共部门对公民的威胁主要来自其高权性，控制权力和保护权利构成传统行政法的核心任务。而随着数字时代的到来，数字技术所带来的风险不仅来自私人部门，而且同样会由公共部门产生。面对公共部门中的数字技术风险，传统行政法中的权力控制和权利保护机制不足以应对，私人部门中的风险规制

〔67〕 参见〔美〕史蒂芬·布雷耶：《打破恶性循环——政府如何有效规制风险》，宋华琳译，法律出版社 2009 年版，第 1 页。
〔68〕 参见高秦伟：《论个人信息保护的专责机关》，载《法学评论》2021 年第 6 期。
〔69〕 参见前引〔62〕，科林·斯科特书，第 9 页。

经验可以发挥重要作用。〔70〕这在不少国家行政管理实践中已经得到印证，公共部门开展风险管理、内部控制和合规管理的现象越来越多，〔71〕在个人信息保护领域尤为明显，这为内部行政法的进一步发展提供了新的素材。

Abstract：The improvement of the personal information protection system in the public sector is the only way to build a digital government ruled by law. China's personal information protection law adopts a declarative legislative model of integrated adjustment of the public and private sectors. At present, it can neither provide sufficient rules and guidance for the protection of personal information in the public sector, nor meet the needs of digital government construction. The construction of personal information protection rules of digital government should not only consider the particularity of the public sector compared with the private sector in personal information processing activities, but also take the innovation of digital government in terms of technology and governance into account, and then formulate special rules. The risk regulation model is not only the trend of personal information protection system worldwide, but also provides a theoretical basis for the integrated adjustment model. Through the proper application of the risk precautionary principle, the risk interpretation and adjustment of personal information rights, the flexible use of risk regulation mechanisms such as risk management, risk communication and risk evaluation, and the joint use of risk regulation strategies such as cooperative governance, independent regulatory institutions, technical governance, responsive governance, experimental regulation and soft law governance, it is the best choice for our country to construct a risk regulation-oriented digital government personal information protection mechanism.

Key Words：digital government, personal information protection, risk regulation

（责任编辑：刘　权　赵建蕊）

〔70〕 Vgl. Englisch/Schuh, Algorithmengestützte Verwaltungsverfahren-Einsatzfelder, Risiken und Notwendigkeit ergänzender Kontrollen, VERW 55 (2022), 155, 189.

〔71〕 Vgl. Stober/Ohrtmann, Compliance: Handbuch für die öffentliche Verwaltung, 2015.