风险预防视角下个人信息保护的范式构建

肖　琪

(中国政法大学 法学院,北京 100088)

摘　要:在数字经济时代,个人信息所面临的多维度风险对个人信息安全乃至国家数字安全构成了严峻挑战,由此催生了风险预防型法治范式的兴起。传统基于赋权的保护范式,因其未能系统考量信息主体的有限理性、个人信息的公共属性以及私法救济的实现困境,导致法律的实效性不足。相较而言,基于风险预防的保护范式关注信息主体的弱势地位、权衡多方主体的利益、凸显信任维系的功能,具有可欲性;还契合国际治理趋势和国内立法导向,具有可行性。为构建个人信息风险预防法律体系,需实施分阶段治理:在初始性预防阶段,通过制度设计和风险监测,形成事前干预机制;在继发性预防阶段,推进行政保护和司法救济双轨前置,强化事中应对机制;在复发性预防阶段,则通过提高行政处罚的确定性和扩大公益诉讼的适用范围,构筑事后威慑机制。

关键词:数字经济;预防型法治;风险预防;个人信息保护;范式

中图分类号:D922.1　　**文献标识码**:A　　**文章编号**:1008-7699(2025)02-0034-10

一、问题的提出

在数字经济时代,大数据技术、生成式人工智能、自动驾驶技术等前沿科技迅速崛起。它们在便利个人生活、提高企业生产效率、促进政府服务效能提升的同时,也引发了严峻的信息安全风险。与传统社会面临的风险相比,当前个人信息[①]面临的风险展现出高度的不确定性、复杂性和隐蔽性,对个人尊严、企业可持续发展乃至国家安全均构成了前所未有的挑战。因此,在数字经济迅猛发展的背景下,如何有效应对信息风险,尤其是如何平衡个人信息保护与数据价值开发,已成为公共政策制定与法学研究的核心课题。

随着我国个人信息保护法律体系的逐步健全,相关研究成果日益丰硕,并伴随着信息技术的飞跃发展持续深化。传统的个人信息保护主要通过赋权路径实现,[②]然而,随着数字化与智能化进程的推进,单纯强调个人控制或私法保护的范式遭遇了诸多挑战。一些学者开始审视个人数据所蕴含的流通价值,并探索基于社会控制、国家义务、结果保护等视角的个人信息保护新范式,旨在平衡个体权益与公共利益。[③]当前,“基于风险”的个人信息保护范式在学界悄然兴起,[④]相关研究仍然显得相对薄弱。例如,数字时代

收稿日期:2024-12-30

作者简介:肖　琪(1997—),男,江西吉安人,中国政法大学法学院博士研究生.

① 本文不严格区分“个人信息”与“个人数据”的概念,两者指涉的对象并无实质差别,只是在应用场景上各有侧重。

② 相关论述参见王利明.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[J].现代法学,2013(4):62-72;程啸.论我国民法典中个人信息权益的性质[J].政治与法律,2020(8):2-14.

③ 相关论述参见高富平.个人信息保护:从个人控制到社会控制[J].法学研究,2018(3):84-101;王锡锌.个人信息国家保护义务及展开[J].中国法学,2021(1):145-166;蔡培如.个人信息保护原理之辨:过程保护和结果保护[J].行政法学研究,2021(5):91-101.

④ 有论者以公益诉讼为切入点,探讨风险社会语境下的个人信息保护,参见董储超.论风险社会视域下个人信息保护公益诉讼的优化进路[J].学术探索,2020(12):117-127.亦有论者基于风险治理、风险控制等视角提出了“基于风险”的范式,旨在克服传统个人信息保护法律制度的结构困境,参见张涛.探寻个人信息保护的风险控制路径之维[J].法学,2022(6):57-71;刘权.风险治理视角下的个人信息保护路径[J].比较法研究,2024(2):62-76.此外,仍有论者指出“基于风险”的保护范式具有一定局限性,参见赵鹏.“基于风险”的个人信息保护?[J].法学评论,2023(4):123-136.

的个人信息权益面临哪些新型风险？传统保护范式呈现出何种局限性？为何需要引入基于风险预防的个人信息保护范式？以及如何有效实现基于风险预防的个人信息保护？这些关键问题还有待进一步探索与明确。

基于现有研究，本文旨在：(1)厘清数字时代个人信息所面临的风险以及传统保护范式遇到的挑战；(2)从理论层面阐释引入风险预防保护范式的正当性；(3)从制度层面构建基于风险预防的个人信息保护规范体系；(4)界定风险预防的限度，强调风险与机遇共存于数字经济时代，应当兼顾个人信息保护与利用。

二、个人信息面临的多种风险及传统保护困境

风险和不确定性是经济活动中的内生性要素，尤其在大数据时代，信息风险的不确定性可能导致系统性后果。因此，首要任务在于系统识别信息安全面临的各种风险。这不仅是保障信息安全的前提和基础，也是解构传统保护范式结构性缺陷的先决条件。

(一)个人信息面临的多种风险

根据个人信息/个人数据在不同阶段所呈现的特征，本文将个人数据管理流程细分为数据收集、数据处理、数据存储、数据共享、数据分析和数据再利用六个阶段。在整个数据管理生命周期中，每个环节都潜藏着信息安全风险。

1.数据收集阶段的风险

在数据收集阶段，用户面临未经授权或超出授权范围收集信息的风险。暂且不论用户通过点击和阅读隐私政策进行授权的有效性，互联网平台企业可以使用多种技术手段获取用户信息，而普通用户往往难以辨别这些行为是否经过授权。即便用户已授权，网络服务提供者也可能过度收集个人信息。

2.数据处理阶段的风险

数据处理是一个紧随数据收集之后的环节，主要涉及信息脱敏、清洗及加工等工作。在此过程中，用户往往面临着“最小必要原则”被虚置及隐私安全遭受威胁的挑战。例如，智能汽车辅助驾驶乃至自动驾驶技术的高效运行，依赖于各类传感器采集的大量数据，这些数据不仅包括车辆内部的用户个人信息，还包括地理信息、环境信息以及路人的敏感信息。若不对这些敏感信息进行严格脱敏并定期删除，可能会严重侵犯他人的肖像权和隐私权，引发用户的隐私焦虑。

3.数据存储阶段的风险

数据存储指将初步处理后的数据通过物理存储介质或云技术进行存储的过程。个人信息可能被永久保留，这不仅可能加剧个体的隐私担忧，也可能构成对用户“被遗忘权”的侵犯。相比于传统硬盘存储，云存储技术能够容纳更大规模的数据，其中所包含的信息既有敏感的身份证照片，也有日常生活的影像记录。换言之，数据易存储、易流通的特性无疑增加了个人信息泄露的风险。

4.数据共享阶段的风险

数据共享是指将数据资源向其他用户或平台开放，供其进行挖掘并开发商机。在数字经济蓬勃发展的当下，数据共享是数据开发与二次利用的基础，也是互联网企业探索新的盈利模式的重要手段。通过数据共享乃至交易，互联网企业或个人能够以较低的成本投入获取高额回报。此外，受限于成本因素以及缺乏有效的正向激励机制，信息主体通常不会对接收方进行严格的资质审查及执行监督。这一现状无疑增加了个人信息被第三方非法利用的风险，进而可能对公共利益造成损害。

5.数据分析阶段的风险

数据分析是深层次的数据处理的过程，侧重于提升数据价值的利用效率。在此阶段，用户可能会面临不同行业的算法歧视，其基本权利与人格尊严可能受到侵犯。[1]例如，在外卖行业中，平台可能通过算法不断压缩骑手的送餐时限，以提升效率；在媒体娱乐领域，个性化推荐看似贴心，但也限制了用户获取

信息的深度和广度,致使“信息茧房”形成;在电子商务领域,部分平台利用大数据算法“杀熟”,在商品价格上实施歧视性差别对待,违反了公平交易原则。

6. 数据再利用阶段的风险

数据的再利用标志着对数据应用的深化,并可能因生成新数据而开启另一轮数据生命周期。在此过程中,用户享有的知情权、处分权、更正权及安宁权等权益,均存在被侵害的风险。例如,个性化广告的推送不仅体现了技术的精确性和服务的个性化,更暴露互联网“勾画一切”的侵略性。再如,以 ChatGPT 及 DeepSeek 等为代表的 AI 产品,其语料库常混杂真伪难辨的个人信息。用户每次交互的信息输入均构成对系统的“数据投喂”,此类信息也存在泄露的风险。[2]

(二)传统保护范式及其实践困境

步入数字经济时代,个人信息面临风险的危害性及信息主体对潜在风险认知的可能性较于以往发生巨变,这为传统的个人信息保护范式带来了挑战。

1. 基于赋权的传统保护范式

通常认为,传统个人信息保护始于个人计算机进入民众的日常生活。20 世纪 70 年代,信息技术的兴起显著降低个人信息处理的成本,推动个人信息数字化。随后,互联网及物联网的崛起,进一步便利了个人信息的数字化存储、复制和传播。然而,大规模的个人信息处理也引发了一系列公平性问题。为了应对这些挑战,美国政府率先发布了《公平信息实践准则》,赋予个人相关权利。此后,公平信息实践理论在个人信息保护领域影响深远,被欧盟及多个国际组织采纳。尽管其具体内容及实施力度因国家或组织而异,但对个体赋权的核心理念始终一致。

我国现行的法律虽未直接将个人信息受保护界定为权利,但《中华人民共和国民法典》(以下简称《民法典》)与《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》)的相关条款均体现了个人信息受法律保护的理念。① 从理论层面,以《民法典》及《个人信息保护法》的酝酿颁布为契机,学界围绕个人信息保护本质属于权利抑或权益展开了深入探讨。② 此种权利话语的理念及主张,不仅在理论上存在泛权利化倾向,也可能导致个人信息保护与传统隐私权保护的功能重叠。传统个人信息保护路径以个人赋权为基本逻辑,以私主体的事后救济为主导,体现个人权利本位的价值取向。然而,随着数字技术全面渗透到社会生活各领域,个人信息风险已逐渐超出传统保护范式的应对范围。

2. 信息主体的认知与决策困境

告知同意制度作为传统个人信息保护范式的基础和核心,面临信息主体认知能力与制度结构的双重困境。一方面,数字鸿沟与信息过载使信息主体在信息决策时面临显著的认知挑战。随着“互联网+”成为常态,数字鸿沟及其衍生的数字弱势群体问题已从学术议题转变为必须面对的社会现实。年龄、学历及地域差异可能加剧数字鸿沟,而随着技术高速发展和教育资源分配不均,个体信息获取及利用能力的差距持续扩大。信息处理领域的“数字鸿沟”尤为突出,数字弱势群体常因隐私政策中的专业术语难以理解,无法基于“意思自治”形成有效同意。即便部分用户能初步理解隐私政策,信息过载引发的同意疲劳仍会导致其在未充分阅读告知内容时草率授权。因此,用户普遍缺乏通过隐私政策全面识别风险的能力,预设信息主体完全理性缺乏现实基础。

另一方面,企业平台与用户间的结构性不平等亦会削弱告知同意制度实效性。实践中,互联网平台企业凭借经济与技术上优势,既可以在隐私政策中设计免责条款以规避风险,又因信息风险的不可预见性,促使用户用信息换便利。此外,平台技术垄断进一步压缩用户的选择权。用户对隐私政策的同意只

① 参见《民法典》第一百一十一条;《个人信息保护法》第四十四至五十条。

② 相关研究参见杨立新. 个人信息:法益抑或民事权利——对《民法总则》第 111 条规定的“个人信息”之解读[J]. 法学论坛,2018(1):34-45;王成. 个人信息民法保护的模式选择[J]. 中国社会科学,2019(6):124-146;周汉华. 个人信息保护的法律定位[J]. 法商研究,2020(3):44-56.

呈现出全有或全无的状态(即不授权就无法使用产品),成为部分用户从不阅读隐私政策的主要原因。①综上,告知同意规则为代表的赋权保护范式存在制度空转和权利虚置的风险。

3.公共属性与保护范式的冲突

数字经济时代,以数据为载体的海量个人信息逐渐成为生产要素,凸显出更强的财产性而非人格性特征。实践中,个人信息保护常与隐私权保护混同,这一混淆不仅存在于公众日常生活,也见于商业领域中。网络服务提供者多将个人信息处理告知书称为隐私政策,然二者存在根本差异。法律规制层面,严重侵犯他人隐私可能招致行政处罚,侵害个人信息安全则可能构成刑事犯罪。民事救济层面,二者虽均可主张侵权救济,但底层逻辑并不相同。我国对隐私权侵害适用过错责任原则,对个人信息安全侵害则采过错推定原则。可见个人信息保护较隐私权保护,呈现出更强的公共属性,也更依赖行政法甚至刑法的救济。

此外,个人信息的适度开放与合理流通有利于营造信任氛围并创造商业价值。例如,网络实名制有助于净化网络环境,失信被执行人黑名单制度能督促法律责任承担。因此,个人信息的处理牵涉到个人、企业和政府多方利益,实现信息的共享已成为时代发展的迫切需求。

4.风险社会下的私法救济受限

贝克关于风险社会具全球化和多元化特征的洞见,[3]为理解数字时代的个人信息风险提供了重要视角。传统的个人信息保护制度依赖事后救济,且以损害后果发生为前提。然而,在信息风险社会,个人信息安全侵害呈现规模性、滞后性和无形性的特点。即便遭受损害,信息主体也难以溯源具体处理者,甚至无法及时止损。此外,信息安全事件通常波及众多信息主体,这使因果关系认定更趋复杂。因此,仅依赖个体诉讼难以有效救济。一方面,鲜有信息主体主动行使法定权利;另一方面,鉴于信息处理技术的高度专业化,信息主体难以取证,司法机关亦难明确侵权主体、因果关系及损害后果。可见,个人信息私法救济存在较大障碍。

综上,赋权保护范式预设了信息主体具备高度理性,可以识别信息风险并作出有效的同意决定,同时能够及时察觉损害并正确地寻求救济。然而,数字技术飞速发展使得传统路径失效。因此,亟需构建一种新的保护范式以适应社会需求。

三、基于风险预防保护范式的理论基础

在当代中国,预防型法治植根于本土预防性治理传统,是本土传统和风险社会、科技革命交互作用的产物。[4]基于风险预防视角构建的个人信息保护范式,能够适应数字经济时代的发展趋势,展现出理论层面的可欲性和规范层面的可行性。

(一)基于风险预防保护范式的可欲性

风险预防的语境下,个人信息保护范式在体现了“根治未病”“未雨绸缪”及“防患于未然”等事前防范的治理理念,然而其理论根基尚待厘清。

1.重构有限理性下的认知框架

构建个人信息保护的理念框架需正视信息主体有限理性,该判断根植于对其弱势地位的深切关怀及对信息风险不确定性的深刻认识。传统完全理性假设认为,个体或者组织在不确定环境中,仍然能够掌握所有信息并在所有的可能选择中找出最优解。此预设既见于主流经济学的理性经济人,亦存于赋权保护范式。西蒙有限理性理论将心理学因素纳入行为人决策分析,揭示了人的真实选择往往只能做到有限的理性。[5]认识到有限理性才是更符合现实的认知框架后,个人信息保护须摒弃理性人假设窠臼。

① 相关数据参见中消协发布《App个人信息泄露情况调查报告》[EB/OL].(2018-08-29)[2024-12-15].https://www.cqn.com.cn/pp/content/2018-08/29/content_6213791.htm.

以有限理性为理念预设,基于风险预防的个人信息保护范式深刻认识到信息主体相对于信息处理者的不对等地位,进而倡导国家和社会提前介入,要求监管机构与信息处理者共同承担个人信息风险管理的义务,同时在此基础上共享信息流转所创造的价值。步入大数据时代,个人信息所面临的风险呈现出高度不确定性和不可逆损害性,使得信息主体往往难以有效地预测风险,且通过个体发起的民事诉讼也难以获得及时救济。因此,风险预防作为一种国家治理策略的调整,其核心在于将防范的重心前置,侧重于对潜在风险的主动干预而非仅局限于对传统损害后果的补救。

2.以价值权衡实现公益价值

在大数据时代,个人信息所承载的个体权益与公共利益存在微妙张力。以数据为载体的个人信息,不仅关联着个人的权利和人格尊严,还具有商业与公共管理价值。[6]然而,基于赋权的保护范式强调个体对信息的控制而非利用效率,这种权利导向思维虽颇具象征性宣示意义,却往往忽视了制度的实际运行效果。在此背景下,基于风险预防的个人信息保护范式应运而生,既注重对数据信息源头治理,也充分认可数据信息的共享和流通价值。这一范式对个人信息的认识不局限于权利归属或以特定主体为中心,而是致力于探索如何在维护信息主体人格尊严的同时,有效实现对数据信息的开发和利用,进而为更多集体性、公共性利益的保护创造空间。

从单一权利本位向综合价值权衡的认知转变,不仅兼顾了各方利益,亦能为风险预防的正当性提供有力支撑。面对信息风险的不确定性,难以将风险预防与事后救济的成本效益进行量化对比,用户的感受与公众的安全也难以简化为数值。通过价值权衡,可以发现风险预防措施能够有效维护信息主体的人格尊严。同时,国家和企业实施的风险治理策略,也可视为一种将事后救济成本转化为事前干预成本的“转移支付”。

3.以事前介入强化信任关系

国家事前介入的深远意义不仅在于弥补事后救济的局限性,更在于营造一种主体间迈向沟通信任的合作生态。互联网和数字技术的发展已然激发了人类天生的分享欲望,个人信息保护的研究也应当顺应这一倾向。构建和维系一种基于信任的社会氛围,不仅有利于社会的整体福祉,更是提供了社会交往的基石,并决定着我们将如何分享自身信息。

在理论研究中,有论者指出,数字时代的信息隐私实际上是一种关于信任而非个人权利的讨论,个人信息保护的对象也应当是信任关系而非个人权利。[7]还有论者提出,应对互联网企业平台施加审慎处理的义务,从而构建一种基于信任的个人信息保护范式。[8]从实践层面看,信息主体对网络平台的信任有利于数据信息的开发和利用。用户从不阅读应用权限和隐私政策的原因除了“不授权就无法使用”之外,主要还是出于对互联网平台企业的信任。① 这也说明,信赖关系对于个人信息保护而言,具有不可估量的价值。[9]因此,国家采取基于风险预防的事前介入策略,积极引导并强化信息处理者承担对个人信息严格保密、审慎处理和忠诚维护的义务,不仅能够有效筑牢个人信息安全防线,还能进一步促进信任关系的稳固建立以及合作互惠格局的形成。

4.风险预防应成为国家法定义务

基于风险预防的个人信息保护范式能够有效应对传统保护范式在数字时代所面临的挑战,更为重要的是,对个人信息安全的风险预防本身就是一种国家义务。“风险”作为一个现代社会特有的概念,②指代一种产生与预期相悖的负面结果的不确定性。在我国的法律实践中,损害或危险往往是国家干预的重要理由。对于已发生的损害,国家的干预毋庸置疑具有正当性;而对于潜在的紧迫危险,侵权法上也提供了“消除危险”的救济途径。而在西方学界,密尔认为只有行为对他人的人身或财产造成损害,国家才提

① 相关数据参见中消协发布《App 个人信息泄露情况调查报告》[EB/OL].(2018-08-29)[2024-12-15].https://www.cqn.com.cn/pp/content/2018-08/29/content_6213791.htm.

② 古人并不认为人类可以自己掌控命运,往往信奉天意或者神意。

供救济予以干预。[10]范伯格则认为损害是一种特殊利益受损的状态，而国家需要处理的干预的是因不法而对利益造成的阻挠、阻碍或破坏。[11]由此可见，传统损害观念的核心要素是已然发生的或者确信会发生的不利益。

另有我国学者认为个人信息风险亦是一种损害，[12]进而主张对信息风险进行法律规制。然而，此论断轻视了损害的确定性和风险的不确定性之间的鸿沟，并不具有强说服力。此外，风险与危险之间同样存在质的差别，危险所指向的是损害发生具有相当确信程度的情况，而风险则蕴含着科学上的不确定性。在贝克看来，风险与危险的来源、因果关系的可证明程度、规模及可感知程度都存在不同。[7]综上所述，不能将风险简单地等同于传统的损害或危险。（见表 1）

表 1　风险与损害、危险的区别

	损害	危险	风险
来源	——	自然环境	人类社会
因果关系	——	可以判断	难以证实
损害的确定程度	已然发生	相当确信	难以确定
应对	报应/填补	危险制止	风险预防

然而，国家对不确定风险的干预，实际上反映的是一种人类社会从危险世界观向风险社会观转变的历史进程，这是人类世界观的一次历史性演进。[13]在数字时代，当信息主体的敏感信息处于失控状态时，隐私焦虑乃至恐惧的情绪极易在社会中弥漫。一旦恐慌情绪开始蔓延，无论其客观依据是否存在，国家都可能需要进行干预。[14]从认知心理学的角度来看，风险的最坏情况本身就足以动摇公众的观念，而至于这一“最糟糕情景”实际发生的可能性大小，实则并非关键因素。[15]简言之，随着科技快速发展，现代社会充满着各种不确定性风险，若仅将具有明确可预见性的“危险”与“损害”作为国家干预的界限，难以有效地维护社会的整体安全。

（二）基于风险预防保护范式的可行性

基于风险预防的个人信息保护范式不仅具有可欲性，也展现出切实的可行性。这一保护范式既符合国际的风险治理趋势，也在国内具有坚实的规范基础。

1. 风险预防的全球趋势

从国际规范制定的角度看，风险预防已然成为个人信息保护立法的核心要素。近年来的趋势表明，风险预防不再仅局限于理念层面，而是已转化为一种切实可行的个人信息保护策略。2014 年，欧盟就发布了《关于基于风险的方法在数据保护法框架中的作用的声明》，并在之后的《通用数据保护条例》多个条款中体现了“基于风险的方法”。① 当前，风险已成为欧盟监管数字技术的一个重要指标。[16]此外，联邦贸易委员会作为美国个人信息保护领域的主要监管机构，也要求对个人信息采取风险评估和风险控制措施。由此可见，基于风险预防的保护范式已成为全球个人信息保护立法领域的重要共识和实践导向。

2. 宪法权利的基本保障

从宪法规范层面来看，《中华人民共和国宪法》第三十三条第三款规定的“国家尊重和保障人权”，为个人信息保护的国家干预提供了坚实的宪法依据。其中，相较“尊重”，“保障”更加强调了国家通过消除或降低风险来保障公民权利的义务。在此语境下，“人权”主要指“人之所以为人”的广义权利范畴，而非狭义范畴的基本权利。因此，无论个人信息保护是否构成基本权利或者一般民事权利，均受国家的保护。此外，该条款还具有制约公权力的深刻内涵，即国家不仅需要防范个人信息遭受他人侵害的风险，还需警惕公权力自身可能成为风险源。因此，预防公权力在行使过程中侵犯个人信息权益，也是国家应尽的义务，这是“尊重”人权原则的必然要求。

① 《通用数据保护条例》（risk-based approach）规定了控制者责任（第 24 条）、通过设计及默认方式保护数据（第 25 条）、保存处理活动记录（第 30 条）、数据保护影响评估（第 35 条）、数据泄露通知（第 33-34 条）等。

3.法律规范的贯彻实施

就法律规范层面而言,①《个人信息保护法》文本中,共有两个条文提及“影响评估”,三个条文使用“风险”一词,还有三个条文明确提出了“安全评估”。尽管该法未明文规定风险预防原则,但相关条款无疑体现了风险预防的理念。一方面,法律区分了“一般个人信息”和“敏感个人信息”的处理规则,实际暗含了对不同风险的分级控制。例如,对于敏感个人信息的处理应当取得单独同意甚至书面同意,严格程序要求体现了对高风险场景的预防性规制。另一方面,法律明确要求“预防和惩治侵害个人信息权益的行为”(第 11 条)。具体而言,国家要求个人信息处理者主动承担个人信息跨境的安全评估(第四十条)、个人信息保护影响评估(第五十五条及第五十六条)及个人信息泄露通知(第五十七条)的义务。

除信息处理者外,履行个人信息保护职责的部门亦承担风险管理职责。随着数据处理流程的深入,用户个体对信息风险的控制能力有限,法律因此赋予职能部门介入权限。《个人信息保护法》第六十一条明确规定了相关职能部门履行组织测评并公布应用程序等个人信息保护情况的职责。此外,第六十四条规定职能部门可按权限和程序约谈存在风险的个人信息处理者或要求其委托专业机构进行合规审计,以消除隐患,降低风险。

四、个人信息风险预防法律体系的构建

基于风险预防的个人信息保护范式不仅具有正当性,也有可行性。本文尝试基于事前(初始性预防)、事中(继发性预防)及事后(复发性预防)三个关键节点,系统探讨如何实现基于风险预防的个人信息保护(见表 2)。在此框架下,遵循受益者和管理者共同负担的原则,基于风险预防的保护范式应当合理地将更多风险注意义务分担至国家和信息处理者。

表 2 风险预防范式下的个人信息保护制度体系框架

	预防性立法	预防性执法	预防性司法	预防性守法
初始性预防(事前)	提高技术标准、强化影响评估	风险监测机制	——	企业的自我规制(全过程构建企业合规激励机制)
继发性预防(事中)	——	行政保护前置化	司法救济前置化	
复发性预防(事后)	——	提高行政处罚的		
可预见性	扩大公益诉讼的适用范围			

(一)源头防控:健全初始性预防规范

初始性预防是一种事前干预策略,旨在从源头上对风险进行监测并及时采取措施,以降低风险,防止损害发生。鉴于司法的相对被动性,本节仅对立法和执法的源头防控功能进行阐释。

1.立法之维

一是构建基于场景化的管理标准体系。鉴于个人信息处理活动具有较高的技术门槛和资金投入要求,且网络产品和服务的应用场景具有多样性,应针对具体场景制定差异化的风险管理标准。例如,配备自动驾驶功能的智能汽车所收集、处理的非敏感区域地理信息和已脱敏的路人信息在技术层面具有正当性,通常不需个人持续的同意。相较之下,医疗机构预约平台或电商平台所收集、处理的信息多涉及个人敏感信息,直接关乎人格尊严和财产安全。因此,应基于信息处理者的行业特征、业务类型及企业规模建立差异化的行政许可制度[17],以确保国家风险管理的有效性。

二是强化个人信息保护影响评估机制。《个人信息保护法》第五十五条和第五十六条初步规定了信

① 据不完全统计,中国现行有效的 305 部法律(截至 2025 年 1 月 1 日)中,包含“预防”或“防范”词汇的专门章节或条款的法律数量超过总量的 1/3,此外还有大量体现预防理念的规范文件难以准统计。

息处理者在何种情形下应当编制个人信息影响评估报告，并明确了报告应包含的内容。2023 年 5 月发布的《网络安全标准实践指南》进一步为网络数据安全风险评估提供了具体指引。在此基础上，可借鉴建设项目环境影响评价制度的经验，适度扩展个人信息保护影响报告的适用范围。根据风险概率和严重程度对影响报告进行分类处理，要求信息处理者编制影响评估报告书、报告表或登记表。此外，还可以要求处理者将影响评估报告与隐私政策置于同一界面向信息主体公示。尽管用户可能不会仔细阅读或难以理解，但该制度设计有助于缩小信息主体与信息处理者之间的信息差，维系双方的信任关系，进而促进数据价值的合理开发。

鉴于短期内修订相关法律可行性较低，且我国立法传统倾向于“宜粗不宜细”，本文倡导的立法侧重于广义的制度设计，旨在推动“行动中的法”的发展，而非频繁修订“书本中的法”。

2. 执法之维

随着科技的快速发展，不可归责于个人且具有规模性和不确定性的风险日益涌现，促使各国立法对政府的授权不再局限于事后救济，而倾向于采取损害发生前的干预措施。在个人信息保护领域，政府的预防性监管已日趋普遍。例如，《个人信息保护法》第 63 条规定，履行个人信息保护职责的部门在履职过程中，有权就个人信息处理活动询问相关当事人并实施现场检查。然而，鉴于信息技术风险通常具有无形性的特征，若行政机关缺乏专业技术支持，将难以及时预警重大风险。因此，有必要依托相关职能部门建立个人信息风险监测机制，具体包括但不限于审查互联网企业隐私政策的合法性及落实情况。尽管多数隐私政策仅照搬法律规定而缺乏实质性内容，但通过持续监测和审查，仍可促使企业切实执行合规的隐私政策。

此外，政府在某些情况下同样可能成为信息风险的来源。在决策或执法的过程中，政府同样涉及对大规模个人信息的处理，一旦出现纰漏，可能构成对个人信息的侵犯。因此，建立政府内部的个人信息风险自我监管机制同样至关重要。

（二）风险遏制：强化继发性预防制度

继发性预防聚焦事中阶段的及时介入，其核心目的在于阻止已经发生的损害继续蔓延或加剧，以最大限度地控制潜在风险及后续影响。在此阶段，除行政机关可提前介入执法外，司法机关也能通过适度的积极作为防范个人信息风险。

1. 推进行政保护前置化

首先，有必要扩大行政强制措施的适用范围。我国法律已授权相关职能部门约谈存在较大风险或已发生安全事件的个人信息处理者。作为较柔性的行政措施，约谈有利于防范风险或损害扩大。对涉嫌违法的个人信息处理所涉设备，主管部门有权查封或扣押，这也是及时止损的有效手段。然而，鉴于数字信息技术的高速迭代及行政机关在信息渠道与技术手段层面的短板，相关职能部门往往难以对实体计算机网络设备进行及时有效的查封。因此，有必要增加行政强制措施类型，如临时下架应用程序、限制新用户注册、关闭信息平台等。

另一方面，应当进一步畅通申诉和投诉渠道。我国相关法律不仅明确了行政机关在损害救济中的职责，也强调了预防重大风险的义务。鉴于信息主体与信息处理者之间的不对等关系，有必要在网络产品或服务中明确标注申诉渠道，以确保双方的有效沟通。此外，考虑到个人信息风险的隐蔽性，还应在信息主体易于获知的网络界面上公布不同网络产品和服务的投诉、举报途径，以便及时引入公权力救济，处理高风险或违法的信息处理活动。例如，强制要求互联网平台企业在隐私政策等网络界面设置在线申诉和投诉选项，这不仅能为行政机关提供重大信息安全风险线索，亦能增强信息主体对互联网平台的信任。

2. 坚持司法救济前置化

鉴于信息主体的弱势地位，应强化检察机关提前介入机制，推动政府和企业主体积极履责，预防损害扩大化。该司法救济前置实践表现为，检察机关通过磋商、听证、检察建议等行政公益诉讼诉前程序，督

促行政机关依法主动履职。最高人民检察院于 2021 年和 2023 年两次发布的 19 件个人信息保护公益诉讼典型案例中,多个案例通过诉前程序即实现有效履责与个人信息保护。故应坚持司法救济前置,进一步完善检察机关与行政机关的协同机制,以构建个人信息多元共治格局。

(三)循环防护:优化复发性预防措施

复发性预防作为一种事后介入策略,系通过惩治措施遏制侵害再次发生。较之传统惩治方式,复发性预防更注重前瞻性和威慑性功能。[18]基于预防理念的事后救济,能够有效实现"个案办理—类案评查(监督)—系统治理"的效果。其双重路径为:一则以惩治力度彰显威慑效能,二则完善公益诉讼,强化处理者监督。

1. 提高行政处罚的可预见性

现行立法对个人信息处理者已设定严厉的刑事责任和责令终止提供服务、高额罚款、吊销行政许可等行政责任。若是这些法律规定仅停留于"书本上的法",则难以形成有效威慑。具有确定性和实效性的惩治措施往往更能促进信息处理者遵守法律。[19]故需细化处罚的裁量基准,建立违法行为严重程度与行政处罚梯度、刑事责任门槛的对应关系,通过提升处罚精准度预防侵害复发。

2. 扩大公益诉讼的适用范围

个人信息风险贯穿于数据处理全生命周期,其隐蔽性和规模性既造成因果关系举证困难,又可能侵害众多信息主体,危及社会公共利益乃至国家数据主权安全。[20]由于个体损害程度轻微,信息主体多缺乏诉讼意愿,即便起诉也难以胜诉。[21]故激活个人信息保护公益诉讼具有必要性。[22]我国虽已建立检察机关为主导的个人信息保护公益诉讼制度,然制度仍需进一步完善。具体而言,个人信息保护公益诉讼不应简单地以人数作为认定的标准,而应当综合考虑风险概率及其潜在影响。另须明确适格社会组织原告地位,完善民事公益诉讼支持机制。综上,扩大个人信息保护公益诉讼的适用范围,既可充分激活风险预防功能,又能弥补传统私法救济不足,进而全方位保障信息安全。

五、结语

赋权模式的个人信息保护范式存在局限性,本文引入风险预防保护范式,通过理论基础和制度构建两个维度,系统阐释其弥补传统保护机制缺陷的价值。相较既往研究,本文以风险预防的关键节点(事前、事中和事后)为纵轴,以法治实践的各个环节(立法、执法、司法和守法)为横轴,构建了一个二维分析框架,系统剖析全过程风险预防范式的实现路径。风险预防范式与赋权范式并非非此即彼的选择题,而是一种合作共存的关系。公共资源的有限性,公权力的绝对干预既不可行,亦会抑制数字经济的发展。数字经济背景下,风险往往与机遇共存,需在认识风险的不确定性与风险预防的基础上,在实践中依据具体情况不断探索和调整预防措施的干预边界。

参考文献:

[1] 马长山,李丹. 数字人权保护的"中国策略"[J]. 法学论坛,2024(5):77-79.

[2] 张新宝. 生成式人工智能训练语料的个人信息保护研究[J]. 中国法学,2024(5):86.

[3] 乌尔里希·贝克. 风险社会:新的现代性之路[M]. 张文杰,何博闻,译. 南京:译林出版社,2018:277.

[4] 黄文艺. 论预防型法治[J]. 法学研究,2024(2):20.

[5] SIMON H A. Administrative behavior[M]. New York: The Free Press,1997: 20-25.

[6] 王禄生. 论法律大数据"领域理论"的构建[J]. 中国法学,2020(2):261.

[7] WALDMAN A E. Privacy as trust: Sharing personal information in the twenty-first century[J]. University of Miami law review,2015(3): 560.

[8] BALKIN J M. Information fiduciaries and the first amendment[J]. U. C. Davis law review,2016(4): 1206-1208.

[9] 刘亚菲. 信息信义关系的法律保护[J]. 法律科学,2025(3):176.

[10] 约翰·穆勒. 论自由[M]. 孟凡礼,译. 桂林:广西师范大学出版社,2011:10.
[11] 乔尔·范伯格. 刑法的道德界限(第一卷):对他人的损害[M]. 方泉,译. 北京:商务印书馆,2013:36.
[12] 田野. 风险作为损害:大数据时代侵权"损害"概念的革新[J]. 政治与法律,2021(10):25-39.
[13] 王旭. 论国家在宪法上的风险预防义务[J]. 法商研究,2019(5):113.
[14] 凯斯·孙斯坦. 风险与理性[M]. 师帅,译. 北京:中国政法大学出版社,2005:1.
[15] 苏宇. 风险预防原则的结构化阐释[J]. 法学研究,2021(1):40.
[16] DE GREGORIO G,DUNN P. The European risk-based approaches: Connecting constitutional dots in the digital age[J]. Common market law review,2022(2): 473-500.
[17] 谭冰霖. 行政处罚的预防目的及其规范建构[J]. 法学研究,2024(6):90.
[18] 罗伯特·考特,托马斯·尤伦. 法和经济学(第六版)[M]. 史晋川,董雪兵,等,译. 上海:格致出版社,上海三联书店,上海人民出版社,2012:188-196.
[19] 赵新潮. 个体权益·公共利益·国家安全:企业数据权利限制的三重考量[J]. 湖北大学(哲学社会科学版),2024(4):143.
[20] 陈晨,李思頔. 个人信息的司法救济——以1383份"App越界索权"裁判文书为分析样本[J]. 财经法学,2018(6):102.
[21] 赵文博. 个人信息保护检察公益诉讼的现实张力与规范完善[J]. 山东科技大学学报(社会科学版),2023(5):52.

Construction of Personal Information Protection Paradigm from the Perspective of Risk Prevention

XIAO Qi

(*School of Law, China University of Political Science and Law, Beijing* 100088, *China*)

Abstract: In the era of the digital economy, the multidimensional risks to personal information pose a serious challenge to the security of personal information and even to national digital security, thus giving rise to the emergence of a risk-prevention rule of law paradigm. The traditional empowerment-based protection paradigm fails to systematically consider the limited rationality of the information subject, the public attributes of personal information, and the dilemma of realizing private law remedies, making it difficult to show the effectiveness of the law. In contrast, the protection paradigm based on risk prevention is desirable because it pays attention to the vulnerable status of the information subject, weighs the interests of multiple subjects, and emphasizes the function of trust maintenance. In addition, it is feasible because it conforms to the international trend and the domestic legislative orientation. Therefore, to build a legal system for the prevention of personal information risks, it is necessary to implement a phased approach to governance: in the initial prevention stage, an ex-ante intervention mechanism is formed through institutional design and risk monitoring; in the secondary prevention stage, the dual-track front of administrative protection and judicial remedies is promoted to strengthen the interim response mechanism; and in the recurring prevention stage, a deterrent mechanism will be constructed after the fact by increasing the certainty of administrative punishment and expanding the scope of public interest litigation.

Key words: digital economy; the preventive rule of law; risk prevention; personal information protection

(责任编辑:董兴佩)