探寻个人信息保护的风险控制路径之维

张 涛

【摘 要】在大数据时代，个人信息保护面临新的威胁和挑战。当前的个人信息保护主要依赖“基于权利的方法”，假定信息主体具有完全理性，赋予信息主体一系列权利，并以“告知—同意”和侵权损害赔偿作为主要的保障机制。实践证明，基于权利的个人信息保护法律制度在大数据时代面临认知和结构困境，个人信息保护需要进行路径重构。“基于风险的方法”承认信息主体的有限理性，将关注点从个体权利的建构转移到信息安全风险的合理分配，已经广泛嵌入新近的个人信息保护法制中。为了在个人信息保护中实施“基于风险的方法”，在自我规制层面，信息处理者应当将“基于风险的方法”融入个人信息保护合规制度体系中，形成“基于风险的合规”；在行政规制层面，个人信息保护专责机关应当通过标准设定、信息收集和行为调节三个方面完善风险规制体系，形成“基于风险的规制”；在司法救济层面，法院可以通过建立风险性损害的识别和评估机制，革新侵权“损害”概念，形成“基于风险的损害”。

【关 键 词】个人信息保护；基于权利的方法；基于风险的方法；风险规制

【作者简介】张涛，清华大学法学院。

【原文出处】《法学》(沪)，2022.6.57～71

【基金项目】本文系2019年国家社科基金重大项目“大数据、人工智能背景下的公安法治建设研究”(19ZDA165)的阶段性研究成果。

在大数据时代，个人信息保护面临新的挑战和困境。[①]现有的个人信息保护立法及实践主要依赖“基于权利的方法”，即通过促进个人信息主体的赋权和能力发展，建构个人信息保护权利体系，进而实现个人信息保护。尽管个人信息保护中“基于权利的方法”契合支配当今权利理论的实践和哲学的观点，即主张“为了使世人相信我们道德理想的‘真理’(道德方面的重要性)，我们需要运用道德术语或权利语言”。[②]然而，“基于权利的方法”主要以工业时代诞生的“公平信息实践原则”为基石，该原则忽视了大数据的运行规律、个体的有限理性、数字经济的发展需求等因素，已经变得“不充分”。这使得“基于权利的方法”虽然能给人“隐私增强”的错觉，但却并未“实际地”为个人提供有效保护。[③]

鉴于“基于权利的方法”之不足，学界也尝试提出了一些替代性或者补充性的解决方案。[④]在风险社会理论下，风险控制的理念和工具被引入个人信息保护中，形成了“基于风险的方法”，其核心是摒弃传统路径中全有全无的“二元化”判断，转而进行“程度性”评估，通过对风险的识别、评估和优先排序，以最小化、监测和控制不幸事件的概率或者影响。[⑤]我国《个人信息保护法》中的一些条款也体现了“基于风险的方法”，如预防个人信息侵害(第11条)、个人信息保护影响评估(第55-56条)等。尽管如此，在理论上，目前鲜有研究成果对“基于风险的方法”进行系统研究，对于如何界定个人信息保护中的“风险”“基于风险的方法”与“基于权利的方法”有何关系、“基于风险的方法”是否具有必要性及可行性等问题，均需要从理论上予以回应。职是之故，本文以国内外已有的个人信息保护法治实践为基础，对个人信息保护中“基于风险的方法”之法理基础进行阐述，在此基础上，提出完善“基于风险的方法”的对策建议，以期为推动我国个人信息保护法治提供借鉴。

一、“基于权利的方法”:个人信息保护的传统路径及其缺陷

当前,个人信息保护的传统路径主要采取“立法赋予权利—信息主体行使权利”的基本逻辑,这契合“基于权利的方法”的核心要素,属于以个人为中心的法律范式。尽管这种方法使得个人信息主体的法律地位得以凸显,但与之配套的权利保障机制却将保护个人信息的主要责任转移给了个人,正如学者所言:“赋予公民以权利,就意味着他们也要负责执行这些权利。”[6]此外,大数据技术的使用不仅对传统以个人为主体的法律保护提出了挑战,而且还造成了难以克服的负担和实践问题。

(一)“基于权利的方法”的核心要素

“基于权利的方法”主要植根于现代权利理论的基本理念与主张。权利的现代基础源于将个体从理性权威和道德权威施加的负担中解放出来,个体仅仅依靠自己,并且越来越占据中心位置,人们开始从个体的优先意义和更重要的现实意义这个角度在现代自然观的语境中思考权利,权利的“主观”概念逐渐成为现代性的一部分。[7]受此影响,“基于权利的方法”最基本的动力之一便是,每个人都是权利持有者(rights-holders),而每项权利都有相应的义务承担者(duty-bearers),应当将公民权利的规范、原则、标准和目标纳入有关个人及社会发展计划的整个过程中。[8]

在理论中,“权利”概念本身具有较大的模糊性,可以通过有关请求、选择、资格、利益或者纯粹的愿景的语言来表达,[9]这导致对“基于权利的方法”的理解也存在差异。根据《联合国关于基于人权的发展合作和规划方法的共同谅解声明》,“基于权利的方法”具有以下核心要素:(1)促进义务承担者的问责制和透明度;(2)促进权利持有者的赋权和能力发展,使义务承担者承担义务;(3)与权利持有者、义务承担者进行合作;(4)确保权利持有者有意义的参与。[10]在“基于权利的方法”中,权利持有者占据核心地位,其有权享有权利、主张权利、追究义务承担者的责任,当然也有责任尊重他人的权利。

(二)个人信息保护中“基于权利的方法”

“基于权利的方法”引入个人信息保护中,不仅深受隐私的权利化传统之影响,而且还与个人信息在信息社会中所蕴含的价值密切相关。从国内外已有的个人信息保护立法看,“基于权利的方法”在个人信息保护中的应用,主要包含三个方面的内容。

1.逻辑前提:信息主体的完全理性。责任理论认为,个人对危险的事物或者情况掌握的信息越准确,其就越有可能就如何因应此类风险做出明智的选择,并且这种选择越有可能符合成本效益和理性。“基于权利的方法”引入个人信息保护中的逻辑前提是假定个人能够自主管理他们的个人信息,即所谓的“个人信息自我管理”或者“个人信息自我决定”,这种逻辑的立论基础是理性选择理论和私法自治原则。在理性选择理论看来,个人信息主体是其自身最大利益的追求者,在特定情境中有不同的策略可以选择,而个人信息主体在理智上相信不同的选择会导致不同的结果,并且在主观上对不同选择结果有不同的偏好排列。[11]在私法自治原则看来,个人信息主体可以根据其自由意志自主形成与他人之间的法律关系,[12]包括禁止或者允许他人收集、存储、分享和使用与之相关的个人信息。

2.基本范式:赋予信息主体法律权利。“基于权利的方法”引入个人信息保护中的基本范式是赋予个人信息主体个人信息权或者个人信息保护权。在理论上,学者们对于个人信息权或者个人信息保护权的法律地位及实现路径有不同的主张,形成了私法上的“隐私权说”“人格权说”“财产权说”等观点和公法上的“基本权利说”等观点。在比较法中,《欧盟基本权利宪章》第8条“个人数据保护”规定,每个人均有权保护有关他或者她的个人数据,由此确立了“个人数据保护权”在欧盟的基本权利地位。[13]在此基础上,欧盟《一般数据保护条例》通过第三章“数据主体权利”赋予了数据主体访问权、更正权、删除权、限制处理权、数据可携带权、反对权等权利。

在我国法律制度中,尽管“个人信息权”或者“个人信息保护权”这一术语并未明确出现在制定法中,但《民法典》和《个人信息保护法》所确立的法律规则却是“基于承认个人信息为受法律保护的一项权利”。[14]《民法典》第111条规定“自然人的个人信息受法律保护”,并在人格权编第六章“隐私权和个人信息保护”第1034~1039条系统规定了个人信息保护

的制度体系，包括知情同意权、查阅与复制权、异议和更正权、删除权等。受《民法典》的影响，《个人信息保护法》第1条立法目的表述为“为了保护个人信息权益……”不过在第四章“个人在个人信息处理活动中的权利”中却通过“个人有权……”的表达方式赋予了信息主体知情权、决定权、查阅权、复制权、更正权、删除权等权利，其中，“告知—同意”是个人信息权利得以实现的首要机制。

3.法律保障：以损害填补为主导的侵权救济。“基于权利的方法”引入个人信息保护中的法律保障是以损害填补为主导的侵权救济。在霍菲尔德权利概念体系中，第一种便是A对B的请求权，此权利相当于B就此项请求的内容而言对于A承担了义务。在基于权利的个人信息保护制度中，信息主体享有个人信息权及附属的知情权、决定权、查阅权等一系列权利，这意味着信息处理者应当承担相应的系列义务。

然而，在实践中，权利的实现和义务的履行并非总是按照立法者预设的图景自主进行。因此，“追究义务承担者的责任”便构成了“基于权利的方法”的核心要素之一。不过，“责任的归结并不是发生于法律的真空之中，而是发生于特殊人际关系和复杂的情境之中”。[15]对个人信息主体而言，只有在信息处理者违反其对信息主体的义务时，信息主体才能追究相应的法律责任。目前，侵害个人信息权利一般适用普通的民事纠纷解决与救济机制，并且主要以侵权责任作为实现路径，这体现在我国《个人信息保护法》第69条的规定中。既然以侵权责任为主导的私法救济成为个人信息权利义务规定得以实现的法律保障机制，那么信息主体在激活这一机制时理应遵循侵权责任的一般原理，尤其是侵权责任的构成要件，即违法行为的存在、损害事实、因果关系和行为人的过错。

(三)基于权利的个人信息保护法律制度之困境

在大数据时代，个人信息的生成、收集、存储、共享、处理和使用均发生了巨大变化，这给基于权利的个人信息保护制度带来了诸多挑战。美国学者丹尼尔·索罗夫认为，一些认知问题破坏了隐私自我管理，导致个人无法作出知情且理性的选择，而由于一些结构问题的存在，导致即使是知情且理性的个人也无法适当地自我管理其隐私。[16]以此为参考借鉴，本文也从认知困境和结构困境两个方面对基于权利的个人信息保护制度在大数据时代面临的挑战进行阐述。

1.认知困境：信息主体难以进行理性选择。如前所述，基于权利的个人信息保护制度倾向于将个人视为理性主体，他们理性地自主决定如何保护或者披露他们的个人信息。根据这种观点，个人是前瞻者、效用最大化者、贝叶斯式的更新者，他们完全知情或者根据已知的随机分布概率作出决定。然而，无论是“理性选择理论”还是“私法自治原则”，其已经被证明存在内在缺陷，难以反映真实的决策场景和理性的心理偏离。个人在行为决策中容易受到“框架效应”“禀赋效应”“现状偏好”等因素的影响，表现出有限理性、有限意志力和有限自利。[17]许多领域的诸多研究发现，即使是在最理想的情况下，全面的信息披露也难以达到其目标，促进个人做出“良好慎重的决策”。[18]

在有关个人信息的决策过程中，个人容易受到多种因素的影响和阻碍，导致难以进行理性选择：第一，不完整的信息会影响个人信息决策，主要体现在三个方面：(1)外部性，当第三方共享有关个人的信息时，他们可能会影响该个人，而该个人并未实际参与这些第三方之间的交易；(2)信息不对称，与个人信息决策相关的信息，可能只有一部分决策方知晓；(3)风险不确定性，受到大数据分类、聚合等特征的影响，个人信息引发的不利影响可以跨越时空，具有强烈的不确定性。第二，即使个人能够获得完整的信息，其可能也无法对大量信息进行处理并采取最佳选择。面对个人信息生成、收集、处理、使用的技术复杂性及后果连锁性，有限理性限制了个人获取、记忆和处理所有相关信息的能力，并使个人容易依赖简化的心理模型、近似的策略和启发式方法。第三，即使个人能够获得完整的信息，并且能够成功地计算出个人信息决策的优化策略，其仍然有可能偏离理性策略。[19]

2.结构困境一：大数据削弱了“告知—同意”机制。在大数据时代，现代数据挖掘和分析技术可能

从以下两个方面削弱“告知—同意”机制的有效性。

第一,大数据的规模效应在客观上限制了信息主体的信息处理能力,同时造成“告知—同意”的形式化。随着社会数字化进程的不断推进,个人的学习、工作和生活均与各种信息技术或者数字设备密切相关,各种隐私政策或者用户协议亦接踵而至。按照美国学者的估计,一名美国互联网用户每年阅读隐私政策的时间成本约为201小时,折合成经济价值约为3534美元,若全体美国公民逐字逐句地阅读在线隐私政策,估计每年损失的时间价值约为7810亿美元。[20]作为“告知—同意”载体的隐私政策给信息主体带来了极大的信息处理负担,导致很多信息主体难以从冗长且充满技术与法律术语的隐私政策中获得有效信息,进而做出明智决定。欧盟委员会报告指出,只有18%的受访者表示完全阅读了隐私政策,49%的受访者表示部分阅读了隐私政策,内容冗长且复杂是不阅读的主要原因,而绝大多数人习惯性地接受同意对话,甚至不看所提供的信息。[21]

第二,大数据下游用途之不确定性不仅导致信息处理者难以制定出完整且明确的隐私政策,也导致信息主体无法对隐私政策进行实质性理解。大数据分析的目的之一便是在数据中找到意想不到的模式和相关性,这意味着无论是信息处理者还是信息主体都不太可能明确知道个人信息将用于发现什么。在大数据世界里,即使是已经“匿名化”或者看起来没有个人身份信息的数据集,也有重新识别的风险,这将破坏以去标识化为条件的个人信息处理同意。[22]

3.结构困境二:大数据导致个人信息私法救济困难。在基于权利的个人信息保护法律制度中,个人若想获得司法救济,主要是通过侵权损害责任为主导的私法救济。在传统侵权法中,“损害”是指“因一定的行为或者事件使某人受侵权法保护的权利和利益遭受不利益的影响”。[23]一般认为,构成“损害”应当具备以下三个要件:一是,损害是侵害民事权益所产生的后果;二是,补救性;三是,客观真实性和确定性。[24]

在大数据时代,与一般侵权造成的损害相比,个人信息权的损害具有以下特征,导致损害事实的认定充满不确定性:(1)分散性。对信息主体而言,其个人信息被众多信息处理者收集、存储、处理和使用已经成为现实,这意味着个人信息侵害行为造成的损害通常涉及不同领域的不同信息处理者;对信息处理者而言,其收集、处理、存储和使用的个人信息可能涉及众多信息主体,这意味着个人信息侵害行为造成的损害通常涉及广泛且异质的信息主体。(2)无形性。在大数据时代,个人信息通常是以电子数据的形式存在,这意味着与之相关的损害通常也是无形的,不同于传统的人身侵害或者财产损失等有形损害。(3)延时性与累积性。个人信息基于其数字化特征,可以进行突破时空的收集、存储、共享和使用,与已经现实发生的损害相比,个人信息损害通常不会立即显现,而是可能随着时间的推移逐渐显现出来。研究表明,在司法实践中,“损害”认定已经成为众多个人数据泄露案件难以通过司法程序获得救济的主要原因之一。[25]

二、“基于风险的方法”:个人信息保护的新路径

囿于时代和制度约束,基于权利的个人信息保护法律制度在大数据时代不可避免地面临困境,其局限性也日益突出,需要超越传统保护路径。无论是在智识上还是“实践”中,“基于风险的方法”之理论视角和实践工具均已日臻成熟。信息主体的有限理性、信息安全风险的合理分配及个人信息保护法风险化的国际趋势,证成了“基于风险的方法”作为个人信息保护新路径的正当性和可行性,我国《个人信息保护法》亦对此作出了积极回应。

(一)何为“基于风险的方法”

随着风险社会的来临,“风险”被作为一个普遍的组织概念加以推广,以提高治理的质量、效率和合理性,其方式远远超过了它与环境保护、食品安全、卫生健康等领域的传统关联。[26]这些“基于风险”的模式、机制、工具被统称为“基于风险的方法”,它们的共同点是:治理不应当以消除所有潜在的损害或者更广泛的“不利后果”为目标;相反,应当关注潜在不利后果的概率及其影响。经济合作与发展组织曾指出,“利用基于风险的方法来设计规制管理和合规战略……可以通过提供更好的危险保护和更有效的政府服务来改善公民福祉”。[27]

尽管不同领域中“基于风险的方法”的基本原理是一致的，但是对规制机构和规制对象而言，“基于风险的方法”具有不同的表现形式及运行机制。对规制机构而言，“基于风险的方法”主要体现为“基于风险的规制”(risk-based regulation)。一般认为，“基于风险的规制”主要有四个特征：(1)风险提供了规制的对象；(2)风险成为规制的正当化依据；(3)风险架构和塑造了规制组织和规制程序；(4)风险塑造了责任关系。[28]对规制对象而言，“基于风险的方法”主要体现为“基于风险的合规”(risk-based compliance)。这种方法侧重于因不合规而产生的风险，并利用对这些风险的评估指导合规工具的选择及资源部署，以最大限度降低风险和提高合规性。[29]

(二)“基于风险的方法”嵌入个人信息保护的正当性

从国内外个人信息保护立法趋势来看，“基于风险的方法”正在重塑个人信息保护法。一方面，对个人信息处理者而言，风险已经广泛融入个人信息保护合规体系中，形成了“基于风险的合规”；另一方面，对个人信息保护监管机构而言，风险已经全面渗透到个人信息保护行政规制中，形成了“基于风险的规制”。结合已有的理论研究和立法实践，本文主要从逻辑前提、现实基础、国际趋势三个方面对“基于风险的方法”嵌入个人信息保护中的正当性和可行性进行阐述。

1.逻辑前提：信息主体的有限理性。“基于风险的方法”嵌入个人信息保护中的逻辑前提是承认个人信息主体的有限理性。在有限理性理论看来，大脑的两个特点奠定了行为与决策的基础：一是，有限的信息处理能力；二是，模块大脑——多重自我与有限自我控制，在存在不确定性的情形中，再多的信息处理也不能解决问题。[30]由于受到有限理性的影响，个人在做出有关个人信息的选择过程中充满了不确定性、模糊性和复杂性。在此种情况下，理论界提出，法律政策需要从“控制范式”转向“保护范式”。这种新的保护范式主要有两个核心特征：第一，强调社会保护，而不是个人控制。换言之，新的个人信息保护范式必须从寻求促进个人对个人信息处理的自我控制，转向授权政府部门对个人信息处理活动是否符合个人利益及社会价值做出选择。第二，强调风险预防，而不是损害填补。申言之，新的个人信息保护范式必须能够保护人们免受以预测分析为代表的大数据技术引发的全部风险，诸如隐私侵害、操纵、偏见、程序不公正等。[31]

个人信息保护中“基于风险的方法”体现了“社会保护范式”的一般原理，即主张由个人控制转向社会保护，但同时又有其独特性：第一，在目标上，“基于风险的方法”承认个人信息主体的有限理性，放弃了“零风险”和“绝对控制”这一不切实际的幻想，转而追求风险的最佳组合。第二，在模式上，“基于风险的方法”要求个人信息处理者和监管机构承担更为重要的风险管理义务，而不是将风险转移给个人信息主体。第三，在方法上，“基于风险的方法”主要通过不同的机制、模式和手段对个人信息保护相关的风险进行识别、评估、分配和管理。第四，在效果上，“基于风险的方法”并非全面改变已有的权利义务内容或者建构一个基于合规的规范性框架，而是更关注“纸面上”的权利义务如何更为实际地体现在个人信息保护实践中，并根据所涉及的风险对信息处理者的义务进行微调。

2.现实基础：信息安全风险的合理分配。“基于风险的方法”嵌入个人信息保护中的现实基础是信息安全风险的合理分配。在现代风险社会中，各种风险类型层出不穷，信息安全风险便是其中之一。随着信息的经济价值和社会价值不断凸显，信息安全风险问题不再是一个单纯的技术问题，而逐渐演变为一个重要的社会问题。这意味着信息安全风险应当成为国家治理的重要内容，治理的理念、方式和工具亦应当根据信息安全风险的特点做出相应的调整，其中一个基本问题便是信息安全风险如何进行合理分配。德国学者乌尔里希·贝克认为：“风险分配的历史表明，风险同财富一样附着在阶级模式之上，只不过是以颠覆的方式：财富在顶层积聚，而风险在底层积聚。”[32]在基于权利的个人信息保护法律制度中，信息安全风险分配尚未达到分配正义的基本要求，甚至通过一些机制将风险不合理地转移给信息主体，产生“有组织地不负责任”现象。

对此，“基于风险的方法”之重要任务就是改变

现有的信息安全风险分配现状，通过“基于风险的规制”和“基于风险的合规”让个人信息处理者承担相对较多的风险。之所以要让个人信息处理者承担更多的信息安全风险，主要理由包括以下几点：第一，信息安全风险主要源于个人信息处理活动，信息处理者是风险的根源。第二，相比个人信息主体，个人信息处理者拥有更多的资源、技术、手段来控制风险。第三，按照风险利益对等原则，个人信息处理者从个人信息处理活动中获益，理应承担更多的风险。第四，让个人信息处理者承担较多的风险，可以刺激其完善自身的个人信息保护合规体系，提升其在“多头执法”背景下的合规“互操作性”，加强问责制、透明度并提升信息处理者的信息保护文化水平。[33]

3. 国际趋势：个人信息保护法的风险化。在风险社会的背景下，鉴于风险管理在其他领域的悠久历史和良好经验，一些国际性规范或者国家(地区)立法已经开始将“基于风险的方法”的理念、机制、工具应用于个人信息(隐私)保护中，作为确保个人信息得到适当处理和个人基本权益获得有效保护的重要手段。

第一，“基于风险的方法”在国际性个人信息保护规范中的体现。在个人信息保护规范体系中，一些国际组织制定的指南或者规则一直占据着重要地位。2013年，经济合作与发展组织对1980年通过的《经合组织个人数据隐私保护和跨境流动准则》进行了修订，其中很多条款均是为了“实施基于风险的方法”。在附带的解释性备忘录中，起草者指出“风险评估在制定隐私保护的政策和保障措施中非常重要”。[34]

第二，“基于风险的方法”在国家(地区)个人信息保护法律政策中的体现。在欧洲，欧盟第29条工作小组于2014年发布了《关于基于风险的方法在数据保护法框架中的作用的声明》，指出应当将基于风险的方法纳入欧盟数据保护法律框架。欧盟《一般数据保护条例》中的诸多条款均是围绕“基于风险的方法”而展开的，如控制者责任(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。

(三)《个人信息保护法》对“基于风险的方法”的回应

尽管在全国人大常委会对《个人信息保护法(草案)》的说明中并未直接体现“基于风险的方法”的相关表述，但是从《个人信息保护法》的具体内容来看，其仍然对“基于风险的方法”进行了回应。

1. 在《个人信息保护法》的保护目标中体现了“基于风险的方法”。我国《个人信息保护法》将“个人信息”分为“一般个人信息”和“敏感个人信息”，并分别对二者的处理规则进行了规定。从处理规则的严格程度看，敏感个人信息的处理规则显然严于一般个人信息，例如，处理敏感个人信息需要单独同意，法律、行政法规授权的情况下，需要书面同意。尽管在通常情况下，对个人信息权益造成的损害往往取决于个人信息处理的具体场景，而不是个人信息本身的内容，但是某些类型的个人信息就其性质而言确实可能对隐私、人格尊严等价值构成严重威胁。因此，从这个意义上看，《个人信息保护法》对“敏感个人信息”的单独且严格规定，实际上隐含了一个先验的、抽离于具体场景的风险推定，即对敏感个人信息的处理可能对个人、群体或者整个社会产生较高的不利影响。

2. 在《个人信息保护法》的保护原则中体现了“基于风险的方法”。在个人信息保护理论与实践中，保护原则一直发挥着重要作用。除了对传统的采集限制原则、目的说明原则、最小必要原则、公开原则等进行规定外，我国《个人信息保护法》还在第11条规定了“风险预防原则”，即“国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为”。在规制理论中，“风险预防原则”一直是风险规制行政的基本原则，亦是“基于风险的方法”的核心要素，它意味着规制机构或者规制对象应当根据该原则设计具体的风险预防机制，并在特定条件下采取相应的风险干预措施。

3. 在《个人信息保护法》的保护机制中体现了“基于风险的方法”。与欧盟《一般数据保护条例》类似，我国《个人信息保护法》也在诸多保护机制中体现了“基于风险的方法”。首先，在个人信息跨境提供方面，《个人信息保护法》第40条规定，对于确需向

境外提供个人信息的关键信息基础设施运营者和处理个人信息达到规定数量的个人信息处理者，应当通过国家网信部门组织的安全评估。其次，在个人信息处理者的义务方面，《个人信息保护法》第55条和第56条规定了“个人信息保护影响评估”，并要求对处理情况进行记录；第57条规定，当发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者要通知监管机构和个人。最后，在个人信息保护的行政规制方面，《个人信息保护法》第61条赋予规制机构对应用程序等个人信息保护情况进行测评的权力，第64条赋予规制机构在发现个人信息处理活动存在较大风险时对个人信息处理者进行约谈的权力。

三、个人信息保护中“基于风险的方法”的完善策略

尽管我国《个人信息保护法对“基于风险的方法”做出了积极回应。然而，相比“基于风险的方法”在其他领域的实践而言，若要充分发挥其在个人信息保护中的潜力，还有大量工作有待探索。从国内外已有的个人信息保护立法框架看，赋予个人信息主体权利、施加个人信息处理者义务和强化个人信息保护规制机构执法共同构成了个人信息保护的三大支柱。[35]以此作为参照，笔者认为，可以从个人信息处理者、规制机构和人民法院三方主体的角度分别提出促进“基于风险的方法”在个人信息保护中有效实施的对策建议，形成“基于风险的合规”“基于风险的规制”和“基于风险的损害”，构建有效的基于风险的个人信息保护法律制度体系。

(一)自我规制：强化信息处理者的风险管理

在规制理论中，自我规制是指“规制对象对自身施加命令和结果的规制，规制对象可以是单个企业，也可以是代表规制对象的行业协会”。[36]就个人信息保护领域而言，个人信息处理者既包括私营部门，也包括政府机构，二者均是《个人信息保护法》的重点规制对象。因此，从自我规制的角度看，应当强化个人信息处理者的风险管理。《个人信息保护法》第58条要求“按照国家规定建立健全个人信息保护合规制度体系”，不过其义务承担者主要限于“提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者”。笔者认为，从保护个人信息和确保合规的角度看，所有的个人信息处理者均应当建立健全个人信息保护合规制度体系，并将“基于风险的方法”融入其中，形成“基于风险的合规”。

至于如何形成基于风险的个人信息保护合规制度体系，则可以充分借鉴风险管理的一般原理及其在其他领域的实践经验。从过程论的视角看，根据国际标准化组织制定的《ISO 31000:2009风险管理——原则和指南》，“风险管理”是指协调活动以指导和控制组织的风险，主要包括建立背景、风险识别、风险分析、风险评估和风险应对等步骤。从构成要素的角度看，风险管理主要包括三个关键要素：(1)人员，在实施技术和操作流程时，组织应当培训合适的人员，以最大限度地提高技术的使用效率，意识、培训和教育是开展风险管理工作的关键。(2)过程，即使用正式的行动序列来实现一个目标。(3)技术，组织应当确保所购买的硬件或者软件符合成本效益，有意义且有效用。[37]以现有理论成果与实践经验作为参考，笔者认为，个人信息处理者可以通过下列举措来完善个人信息风险管理制度体系，强化自我规制，提升合规性。

1.为个人信息风险管理提供组织支持。风险管理是一项复杂的、系统性的、多方面的活动，需要整个组织的参与。从为组织提供战略眼光和高层目标的高级领导或者行政人员，到执行和管理项目的中层领导，再到第一线操作支持组织任务或者业务功能的信息系统的个人，均在风险管理体系中扮演着重要角色。具体到个人信息风险管理，个人信息处理者应当从以下几个方面提供组织支持：首先，应当将个人信息风险管理与组织在其他领域的风险管理方法相结合，确保个人信息风险管理可以利用组织已经投入其他领域的风险管理资源，提高个人信息风险管理的效率。其次，应当制定和完善内部的个人信息风险管理规范和指南，并将其与组织章程或者员工行为守则等规范结合起来。再次，应当任命专门的人员或者组建专门的机构全面负责个人信息风险管理，具体模式既可以采用欧盟《一般数据保护条例》规定的“数据保护官制度”，也可以采用我国《个人信息保护法》规定的“个人信息保护专责负责

人制度”。最后,应当提供个人信息风险管理所需的资源(物力、人力及财力),加强对一线技术人员的专业培训,在组织内部形成个人信息保护的氛围和文化。

2.合理确定个人信息风险管理的目标。风险管理的目标是尽可能全面地减少风险,并明确剩余风险以及如何管理这些风险。我国《个人信息保护法》第51条规定,个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等,采取不同的措施。由此可知,个人信息风险管理事实上与公法中的“比例原则”密切相关,其主要目标是依据不同的风险等级采取“适当的”保护措施,并非“一刀切”地实现“零风险”。个人信息处理者可以根据风险在合规光谱上的不同位置设定不同目标:首先,对于严重性和可能性均很高的风险,必须通过实施安全措施来避免或者减少,以降低其严重性和可能性。其次,对于严重性高但可能性低的风险,必须通过实施安全措施来避免或者减少,以降低其严重性或者可能性,重点必须放在预防措施上。再次,对于严重性低但可能性高的风险,必须通过实施安全措施来降低其可能性,重点强调恢复措施。最后,对于严重性和可能性均比较低的风险,其社会容许性相对较高,尤其是对其他风险的处理也可以一并解决此类风险,因此可以仅将此类风险作为日常监测目标。

3.完善个人信息保护影响评估制度。风险评估是所有领域中风险管理的关键组成部分,比较成熟的环境影响评估便是其典型代表。在个人信息保护领域,风险评估已经从传统的“隐私影响评估”发展成为“数据保护影响评估”或者“个人信息保护影响评估”,并且被视为是“基于风险的方法”在个人信息保护领域的集中体现。我国《个人信息保护法》充分吸收了已有的立法及实践经验,分别在第55条和第56条对个人信息保护影响评估的“适用情形”和“具体内容”进行了规定,初步回答了“什么时候进行个人信息保护影响评估”和“个人信息保护影响评估涉及什么”这两个问题。

与环境保护影响评估以及欧盟的数据保护影响评估相比,我国个人信息保护影响评估制度仍然较为粗疏,其在实践中的效果仍然有待检验。从制度建构的角度看,笔者认为,还应当从以下几个方面对个人信息保护影响评估制度进行完善:首先,应当确定个人信息保护影响评估中“影响”的具体含义。目前,《个人信息保护法》并未明确“影响到底是什么”,这需要个人信息处理者去完成。笔者认为,个人信息处理者可以通过制定“损害清单”的形式对“影响”进行类型化:(1)有形损害,通常是有形的或者经济的,包括人身伤害、丧失行动自由、经济损失等;(2)客观评估的无形损害,主要包括对言论等自由的寒蝉效应、名誉损害、个人恐惧或者焦虑、歧视、污名化等;(3)社会损害,主要包括社会信任丧失、政府权力滥用等。其次,应当完善个人信息保护影响评估的基本程序。个人信息保护影响评估可以由组织内部或者外部的其他人来完成,但是信息处理者必须对该任务负最终责任。此外,在适当的情况下,应当向不同专业的独立专家(律师、IT专家、安全专家、伦理专家等)征求意见,并听取个人信息主体的意见。最后,有必要主动公开个人信息保护影响评估的结果。尽管《个人信息保护法》并未明确信息处理者是否有义务公开个人信息保护影响评估结果,但从促进信任和透明度的角度看,笔者认为,个人信息处理者有必要公开个人信息保护影响评估结果,在形式上可以选择公布摘要或者结论。

(二)行政规制:迈向专责机关的风险规制

行政规制是个人信息保护的三大支柱之一,“个人信息处理规则本质上是国家建立的一套公法秩序,应主要通过监管和公共执行机制予以保障和纠偏”。[38]随着风险社会和规制国家的交织演进,风险规制逐渐成为政府规制的重要内容,也是《个人信息保护法》“风险化”的重要表现。长期以来,我国个人信息保护行政规制一直呈现“九龙治水”的发展态势,存在目标弱化、主体分散、措施乏力和程序模糊等问题,[39]尚未发挥其在个人信息保护中的支柱性作用。我国《个人信息保护法》第6章虽然对个人信息保护规制机构的职责、职权等内容进行了规定,但是仍然没有改变多头执法的现状,并且在执法方式上仍然偏重于事后规制(如行政处罚)。对此,从促进统一规制和部门协调的角度出发,应当设立个人信息

保护专责机关，充分发挥行政组织在风险规制中的作用。在规制理论中，一般认为，风险规制包含三个要素：标准制定、信息收集和行为调节。[40]笔者认为，可以通过采取以下措施来完善个人信息保护专责机关的风险规制。

1.制定个人信息保护具体规则和技术标准。“在任何一个规制体系中，各类标准都有着重要地位。从最广义的角度而言，标准包括规范、目标、任务及规则，规制体系正是据此得以形成。”[41]我国《个人信息保护法》第62条规定，国家网信部门统筹协调有关部门制定个人信息保护具体规则、标准。在未来，我国设立个人信息保护专责机关后，相应的权力也可以由该机关来行使。个人信息保护专责机关在制定具体规则和技术标准时，可以从以下两个方面切入：

第一，应当按照“场景完整性”理论，根据不同的场景制定相应的个人信息保护具体规则和技术标准。从理论上看，在一个单一的综合性法律框架中对个人信息保护的基本原则、权利义务关系、法律责任等内容进行规定，可以最大限度地凝聚社会共识，推动形成个人信息保护文化，促进个人信息保护执法统一。然而，“书本上的法律”并不总是能够成为或者类似于“行动中的法律”。在个人信息保护法中，这种差距尤为明显，而这一问题又因扩大个人信息保护法以试图解决所有新挑战变得更加严重。对此，笔者认为，规制机构应当努力破除“一部法律包打天下”的理念，按照“场景完整性”理论，根据不同领域、不同群体、不同技术的特征制定相应的个人信息保护具体规则和技术标准，推动书本上的法律成为行动中的法律。

第二，应当坚持“技术制衡技术”的理念，充分发挥技术标准在个人信息保护中的规制作用，推动实现“通过设计与默认保护个人信息”。在风险规制中，技术标准一直发挥着重要作用，它不仅可以发挥行为规范作用，而且能在规制机构与规制对象之间提供一个“对话空间”。[42]在个人信息保护领域，随着物联网、人脸识别、算法、云计算等技术广泛融入个人信息的收集、存储、处理和使用中，导致个人信息保护问题变得更为复杂。若仅仅着力于建构基于规范的合规框架，可能并不能解决实际问题，原因在于：许多信息系统、应用程序一旦投入使用后，若仅通过事后的执法与处罚，不仅可能增加规制机构的执法成本，而且可能导致信息处理者因整改成本过高而消极应对存在的问题，这也是目前手机应用程序中个人信息保护问题屡查屡犯、屡禁不止的重要原因之一。对此，规制机构应当统筹协调标准化机构制定技术标准，将个人信息保护法的要求“代码化”或者“技术化”，融入个人信息处理系统、程序的设计中，实现“通过设计及默认保护个人信息”。[43]

2.完善个人信息保护风险规制中的信息收集机制。信息不对称不仅是市场失灵的重要原因，而且是规制失灵的关键诱因，因此，信息收集是所有规制体系的核心，尤其是在以风险的可能性和严重性为关注重点的风险规制中。在规制实践中，规制机构可以通过多种方式收集有关风险的信息。例如，规制机构可以自己进行分析和实验，可以对他人提出报告、测试或者备案注册的法律要求，也可以通过向他人付费获得信息，还可以由投诉人或者举报人自愿提供信息。[44]通常情况下，风险规制中的信息收集需要综合运用上述方法。在个人信息保护领域中，围绕各类新兴技术的乌托邦式和反乌托邦式的言论甚嚣尘上，规制机构需要拨开盲目乐观和过度恐惧的迷雾，发现更为细致和微妙的变化，如此才能制定出符合技术发展规律的规制策略。

第一，完善投诉举报制度。既要通过畅通渠道、给予奖励等方法完善个人信息处理违法的公众举报制度，同时也要完善内部“吹哨人”保护制度。为了避免大量投诉举报带来执法压力，规制机构还需要完善配套的投诉举报处理机制，可以将“基于风险的方法”运用于投诉举报处理中，根据以下几项标准来选择要处理的投诉：(1)严重违法行为；(2)结构性违法行为；(3)涉及许多人的违法行为；(4)可以利用执法工具进行有效干预的违法行为；(5)年度执法重点或者专项执法范围内的违法行为。

第二，建立制度化的技术检测机制。个人信息保护问题带有强烈的技术性和隐蔽性，有些问题需要专业的技术检测才能发现。目前，技术检测已经被广泛运用于App个人信息保护专项治理中。在未来，规制机构应当总结经验，形成制度化、长效的技

术检测机制，对手机应用软件、移动智能终端设备操作系统进行定期合规检测和事后抽查，形成实名登记、监测跟踪、违规处置、信息披露的全流程监管。

第三，建立个人信息保护影响评估强制报告制度。目前，《个人信息保护法》虽然规定了个人信息保护影响评估制度，但并未明确规制机构在影响评估中的作用。若将个人信息保护影响评估完全交由信息处理者进行自由裁量，可能达不到预期的效果。[45]对此，笔者认为，可以借鉴环境影响评估制度的经验，要求信息处理者必须将个人信息保护影响评估结果提交给规制机构，形成“强制性自我规制”。

3.健全个人信息保护风险规制中的行为调节机制。在风险规制中，行为调节亦至关重要，且经常引发争论。在理论上，学术界提出了两种不同的行为调节机制：一种是“威慑式规制策略”，强调对违反规则行为的制裁；另一种是“遵从式规制策略”，强调合作而非对抗，通过协商、劝说或者教育，推动规制对象产生遵从文化。[46]实践表明，无论是单独适用威慑式规制策略还是遵从式规制策略，均存在局限性。因此，一些规制学者指出，应当采取一种混合方法，即所谓的“回应性规制”，其核心主张是：规制要对行业结构做出回应，因为不同的结构将有利于不同程度和形式的规制；规制机构应当对规制对象的不同动机做出调整；有效的规制应当与规制对象、行业协会及其组成人员的不同目标对话。[47]在个人信息保护领域，不同类型、不同规模的规制对象交织在一起，既有公共部门，也有私营部门，具有不同的动机和能力；技术更新迭代较快，且不同行业之间存在异质性，规制问题也比较复杂。因此，笔者认为，个人信息保护专责机关应当充分借鉴回应性规制的核心主张，同时结合我国事前、事中和事后全过程规制的实践经验，从以下几个方面健全行为调节机制。

第一，通过事前咨询、教育和指导等措施加强事前规制。在事前规制环节，重点是对风险进行预防，同时为事中事后规制收集信息。目前，在个人信息保护规制实践中，教育和指导等较为柔性的规制措施已经广泛实施，其集中体现为行政约谈，并且已经被《个人信息保护法》第64条所规定。除此之外，笔者认为，有必要借鉴欧盟《一般数据保护条例》第36条规定的“事先协商”制度，建立“事先咨询”制度，要求提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者在实施个人信息处理活动之前，应当就合规制度体系建设、影响评估等事项向个人信息保护专责机关进行事先咨询，听取规制机构的指导意见。

第二，通过构建执法工具金字塔完善事中规制。在事中规制环节，重点是要对风险进行发现和回应，督促规制对象在合规轨道上运行。在回应性规制理论中，一个重要的工具便是建立“执法金字塔”，根据不同的情形采取干预强度不同的规制措施。在我国当前的规制实践中，无论是“双随机，一公开”还是“基于信用的监管机制”，均充分体现了回应性规制的核心主张。例如，在“基于信用的监管机制”中，其核心逻辑便是根据规制对象的信用风险高低，采取不同干预强度、不同检查频率的差异化规制措施，包括风险提示、信用教育、行政约谈、警告、罚款、吊销证照等。笔者认为，可以考虑将信用风险分级分类规制与个人信息保护相结合，对不同规模、不同类型的规制对象采取不同的规制措施，确定监督执法的优先事项。

第三，通过完善命令—控制措施健全事后规制。在事后规制环节，重点是对违法行为进行纠正，同时对未来的潜在违法行为进行威慑，以行政处罚为代表的命令—控制措施一直是事后规制的核心工具。我国《个人信息保护法》第66条对事后规制中的行政处罚进行了规定，包括警告、没收违法所得、责令暂停或者终止提供服务、罚款等。从内容上看，《个人信息保护法》第66条仅仅为规制机构提供了一个“工具箱”，并未就如何使用工具提供指引。换言之，对何种违法行为应当采用何种类型的行政处罚，《个人信息保护法》并未作出明确规定。笔者认为，尽管从回应性规制的角度看，命令—控制型措施通常属于“高阶工具”，处于备而不用的状态，但是从规制执法的可操作性和企业合规的可预期性角度看，应当制定类似于《个人信息保护行政处罚规定》的具体规则，按照“回应性规制”的核心原理，专门就不同违法行为的构成要件、表现形式、法律责任等进行具体规定。

(三)司法救济:将风险作为一种可补偿的损害

从广义上看,诉讼和行政规制均属于规制体系的组成部分,前者主要由私人民事诉讼在事后触发,由法院主导整个过程;后者主要由政府部门在事前、事中和事后行使行政权力来完成。因此,从这个意义上看,在基于风险的个人信息保护法律制度中,诉讼也可以发挥重要的规制作用。不过,传统以损害为基础的侵权责任救济机制在大数据时代或大规模侵权时代面临困境,侵权法亟待进行范式重构,需要从损害赔偿转变为风险成本分担。[48]在个人信息保护中,为了充分发挥诉讼在救济权利和规制行为方面的作用,有必要将未来风险作为一种"可认知的损害"。[49]事实上,个人信息保护中风险性损害的认定实际上是将"基于风险的方法"融入传统的侵权损害分析框架中,笔者认为,可以从以下两个方面进行完善。

1.识别风险性损害。关于个人信息侵权的风险性损害样态,我国《个人信息保护法》并未提供相应的指引,还有待立法或者司法实践进一步探索。在比较法中,欧盟《一般数据保护条例》在"鉴于条款"(Recital)第75条将"对自然人权利和自由带来的风险"类型化为客观的、物质的或者非物质的损害,具体表现为:个人数据处理可能导致歧视、身份盗窃或欺诈、财产损失、名誉损害、个人数据丧失专业保密性、匿名数据未经授权的去匿名化,及其他显著的经济或者社会危害。在理论上,我们可以将风险性损害分为个人信息暴露导致的风险升高、预防风险的支出和风险引发的焦虑,[50]为司法裁判提供指引。

2.评估风险性损害。在司法实践中,法院之所以对"风险作为损害"这类观点持保守态度,可能主要有以下两点顾虑:一方面,法院担心难以对风险进行可操作的量化评估;另一方面,法院担心原告可能据此提起大量诉讼,进而阻碍数字经济发展和科学技术创新。从其他领域的风险管理经验来看,风险性损害确实难以进行精确测量,但是仍然存在可以测量和量化的因素。事实上,法院在评估风险性损害时的核心逻辑是:当面对某一类风险性损害时,作为理性的个人是否会采取预防措施,如果是,则根据这些措施的合理成本来评估损害。法官在评估风险性损害时,可以考虑以下四种因素:一是,未来损害的可能性和严重程度;二是,数据敏感性和数据暴露;三是,缓解措施;四是,预防措施的合理性。[51]

四、结语

在大数据时代,个人信息保护是维护人的自主性的关键,[52]这在理论上已经基本形成共识。因此,"基于权利的方法"理所当然地成为个人信息保护的首选,而事实也证明,"基于权利的方法"确实在个人信息保护中发挥了至关重要的作用,诸如被遗忘权、数据可携带权、反对权等权利的确立确实给个人信息保护注入了新的生机与活力。然而,"基于权利的方法"在大数据时代面临不可避免的困境,过度强调和依赖这种方法可能并不利于个人信息保护,这便是"基于风险的方法"得以嵌入个人信息保护的重要前提。事实上,"基于权利的方法"与"基于风险的方法"并非两种截然不同的立场,二者本质上是相互关联的。"基于风险的方法"之最终目标是为了保护个人信息权利,而诸如被遗忘权、反对权等权利本质上也是对个人信息风险的回应。因此,本文主张超越传统的个人信息保护路径,并非抛弃确立个人信息权利这一基本立场,相反,"超越"的前提恰恰是承认"基于权利的方法"之合理成分。[53]换言之,"基于权利的方法"并非另造车轮,未来的重要课题是如何将"基于权利的方法"和"基于风险的方法"进行更好融合,为个人信息保护提供更有力的支撑,维护个人在数字时代的尊严与自由。

注释:

①参见[荷兰]玛农·奥斯特芬:《数据的边界:隐私与个人数据保护》,曹博译,上海人民出版社2020年版,第45-52页。

②[美]加里·B.赫伯特:《权利哲学史》,黄涛、王涛译,华东师范大学出版社2020年版,第446页。

③See Fred H. Cate, The Failure of Fair Information Practice Principles, in Jane K. Winn ed., Consumer Protection in the Age of the "Information Economy", Ashgate Publishing Limited, 2006, p. 342.

④参见高富平:《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84页。

⑤参见范为:《大数据时代个人信息保护的路径重构》,载《环球法律评论》2016年第5期,第98页。

⑥ Bart van der Sloot & Sascha van Schendel, Procedural Law for the Data-Driven Society, Information & Communications Technology Law, Vol. 30, No. 3, 2021, p. 324.

⑦参见[美]加里·B.赫伯特:《权利哲学史》,黄涛、王涛译,华东师范大学出版社2020年版,第121-122页。

⑧See Hans Peter Schmitz & George E. Mitchell, The Other Side of the Coin: NGOs, Rights-Based Approaches, and Public Administration, Public Administration Review, Vol. 76, No. 2, 2016, p. 252-262.

⑨参见[美]朱尔斯·科尔曼、斯科特·夏皮罗主编:《牛津法理学与法哲学手册》(上册),杜宴林、朱振、韦洪发等译,上海三联书店2017年版,第525-528页。

⑩See UNDG, The Human Rights Based Approach to Development Cooperation Towards a Common Understanding Among UN Agencies(2003), https://unsdg.un.org/sites/default/files/6959-The_Human_Rights_Based_Approach_to_Development_Cooperation_Towards_a_Common_Understanding_among_UN.pdf, last visit on March 7, 2022.

⑪参见[美]乔恩·埃尔斯特:《解释社会行为:社会科学的机制视角》,刘骥、何淑静、熊彩等译,重庆大学出版社2019年版,第183-184页。

⑫参见黄茂荣:《法学方法与现代民法》,中国政法大学出版社2001年版,第484页。

⑬See Gloria Gonzalez Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer, 2014, p. 2.

⑭申卫星:《论个人信息权的构建及其体系化》,载《比较法研究》2021年第5期,第3页。

⑮[美]朱尔斯·科尔曼、斯科特·夏皮罗主编:《牛津法理学与法哲学手册》(下册),杜宴林、朱振、韦洪发等译,上海三联书店2017年版,第609页。

⑯See Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, Harvard Law Review, Vol. 126, No. 7, 2013, p. 1880-1903.

⑰参见[美]凯斯·桑斯坦主编:《行为法律经济学》,涂永前、成凡、康娜译,北京大学出版社2006年版,第16页。

⑱[美]欧姆瑞·本·沙哈尔、卡尔·E.施奈德:《过犹不及:强制披露的失败》,陈晓芳译,法律出版社2015年版,第43-44页。

⑲See Alessandro Acquisti, Jens Grossklags, Privacy and Rationality: A Survey, in Katherine J. Strandburg, Daniela Stan Raicu eds., Privacy and Technologies of Identity: A Cross-Disciplinary Conversation, Springer, 2006, p. 17-18.

⑳See Aleecia M. McDonald, Lorrie Faith Cranor, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society, Vol. 4, No. 3, 2008-2009, p. 543-568.

㉑See Tuukka Lehtiniemi1, Yki Kortesniemi, Can the Obstacles to Privacy Self-management Be Overcome? Exploring the Consent Intermediary Approach, Big Data & Society, Vol. 4, No. 2, 2017, p. 1-11.

㉒See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review, Vol. 57, No. 6, 2010, p. 1701-1778.

㉓王利明:《侵权行为法归责原则研究》,中国政法大学出版社1997年版,第361页。

㉔参见张新宝:《中国侵权行为法》(第2版),中国社会科学出版社1998年版,第93页。

㉕See Sasha Romanosky, David A. Hoffman, Alessandro Acquisti, Empirical Analysis of Data Breach Litigation, Journal of Empirical Legal Studies, Vol. 11, No. 1, 2014, p. 74-104.

㉖参见[英]罗伯特·鲍德温、马丁·凯夫、马丁·洛奇主编:《牛津规制手册》,宋华琳、李鸽、卢超等译,上海三联书店2017年版,第339-340页。

㉗OECD, Risk and Regulatory Policy: Improving the Governance of Risk, OECD Publishing, 2010, p. 15.

㉘参见[英]罗伯特·鲍德温、马丁·凯夫、马丁·洛奇主编:《牛津规制手册》,宋华琳、李鸽、卢超等译,上海三联书店2017年版,第340页。

㉙See Andrew Haynes, The Effective Articulation of Risk-Based Compliance in Banks, Journal of Banking Regulation, Vol. 6, 2005, p. 146-162.

㉚参见[美]阿兰·斯密德:《冲突与合作——制度与行为经济学》,刘璨、吴水荣译,上海人民出版社2018年版,第29-30页。

㉛See Dennis D. Hirsch, From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics, Maryland Law Review, Vol. 79, No. 2, 2020, p. 461-462.

㉜[德]乌尔里希·贝克:《风险社会:新的现代性之路》,张文杰、何博闻译,译林出版社2018年版,第25页。

㉝参见田野:《风险作为损害:大数据时代侵权"损害"概念的革新》,载《政治与法律》2021年第10期,第30页。

㉞OECD, The OECD Privacy Framework, OECD Publishing, 2013, p. 12.

㉟See Andra Giurgiu & Tine A. Larsen, Roles and Powers of National Data Protection Authorities, European Data Protection Law Review(EDPL), Vol. 2, No. 3, 2016, p. 342-352.

㊱[英]罗伯特·鲍德温、马丁·凯夫、马丁·洛奇主编:《牛津规制手册》,宋华琳、李鸽、卢超等译,上海三联书店2017年版,第167页。

㊲See Corey Schou, Steven Hernandez, Information Assurance Handbook: Effective Computer Security and Risk Manage-

ment Strategies, McGraw-Hill Education, 2015, p. 76.

㊳王锡锌:《个人信息权益的三层构造及保护机制》,载《现代法学》2021年第5期,第119页。

㊴参见邓辉:《我国个人信息保护行政监管的立法选择》,载《交大法学》2020年第2期,第140页。

㊵See Christopher Hood, Henry Rothstein, Robert Baldwin, The Government of Risk: Understanding Risk Regulation Regimes, Oxford University Press, 2001, p. 23.

㊶[英]罗伯特·鲍德温、马丁·凯夫、马丁·洛奇主编:《牛津规制手册》,宋华琳、李鸽、卢超等译,上海三联书店2017年版,第115页。

㊷参见关保英:《论行政法中技术标准的运用》,载《中国法学》2017年第5期,第216页。

㊸张涛:《大数据时代"通过设计保护数据"的元规制》,载《大连理工大学学报(社会科学版)》2021年第2期,第79页。

㊹See Christopher Hood, Henry Rothstein, Robert Baldwin, The Government of Risk: Understanding Risk Regulation Regimes, Oxford University Press, 2001, p. 24.

㊺See Maria Eduarda Gonçalves, The Risk-Based Approach under the New EU Data Protection Regulation: A Critical Perspective, Journal of Risk Research, Vol. 23, No. 2, 2020, p. 142-144.

㊻参见[英]罗伯特·鲍德温、马丁·凯夫、马丁·洛奇主编:《牛津规制手册》,宋华琳、李鸽、卢超等译,上海三联书店2017年版,第134-135页。

㊼See Ian Ayres, John Braithwaite, Responsive Regulation: Transcending the Deregulation Debate, Oxford University Press, 1992, p. 4.

㊽参见刘水林:《风险社会大规模损害责任法的范式重构——从侵权赔偿到成本分担》,载《法学研究》2014年第3期,第109页。

㊾See Daniel J. Solove, Danielle Keats Citron, Risk and Anxiety: A Theory of Data-Breach Harms, Texas Law Review, Vol. 96, No. 4, 2018, p. 737-786.

㊿参见田野:《风险作为损害:大数据时代侵权"损害"概念的革新》,载《政治与法律》2021年第10期,第34-35页。

(51)See Daniel J. Solove, Danielle Keats Citron, Risk and Anxiety: A Theory of Data-Breach Harms, Texas Law Review, Vol. 96, No. 4, 2018, p. 774-775.

(52)See Paul Bernal, Internet Privacy Rights: Rights to Protect Autonomy, Cambridge University Press, 2014, p. 12.

(53)参见张守文:《经济法责任理论之拓补》,载《中国法学》2003年第4期,第15页。

Exploration on Path of Risk Control of Personal Information Protection

Zhang Tao

Abstract: In the era of big data, personal information protection faces new threats and challenges. The current personal information protection mainly relies on the "rights-based approach", which assumes that the information subject is fully rational, grants a series of rights to information subjects, and uses "inform-consent" and harms for infringement as the main guaranteed mechanism. Practice shows that the rights-based legal system for personal information protection faces cognitive and structural dilemmas in the era of big data, and a methodological shift is needed for personal information protection. The "risk-based approach", which recognizes the limited rationality of information subjects and shifts the focus from the construction of individual rights to the reasonable allocation of information security risks, has been widely embedded in the recent legal system of personal information protection. To implement the "risk-based approach" in personal information protection, at the level of self-regulation, information processors should integrate the "risk-based approach" into the compliance system of personal information protection to form the "risk-based compliance"; the agency responsible for personal information protection should improve the risk regulation system through three aspects: standard setting, information collection and behavior adjustment, and form a "risk-based regulation"; at the level of judicial regulation, the court can establish risky harms identification and the evaluation mechanism, innovate the concept of "harms" in infringement, and form "risk-based harms".

Key words: personal information protection; rights-based approach; risk-based approach; risk regulation

