我国数据安全风险治理中DPIA的应用与完善

高润青
(中国政法大学 法学院,北京 100088)

[摘　要]在数据安全风险治理中,DPIA的制度定位为事前数据风险评估和数据控制者的自我规制者。我国在个人信息保护法中规定了DPIA,其在数据安全风险治理中的应用价值体现在事前预防修正和事后救济、自我规制降低治理成本和技术治理补足法律治理等方面。随着智能科技日新月异的发展,DPIA在数据安全风险治理中的应用困境也日益显现,表现为应用场域泛化可能、自我规制软化倾向与事前预防和事后归责失联等三方面。鉴于此,文章以建构开放型DPIA程序为视角,提出根据风险程度精确应用场域、保证评估全流程的开放透明、构建内外兼容的协同治理、衔接事前预防和事后归责等四方面的举措。

[关键词]数据安全;DPIA程序;风险治理
doi:10.3969/j.issn.1673-9477.2024.03.012
[中图分类号]F49　[文献标识码]A　[文章编号]1673-9477(2024)03-0085-08

在数据治理的背景下,数据处理行为很可能涉及个人敏感信息,产生大规模使用和系统性监控,且利益诱因很可能诱使数据处理者将数据于治理目的之外使用。倘若数据控制者利用自动化决策等新技术工具突破数据处理目的,将收集的数据挪作他用,势必会危及数据主体的权利实现。基于对数据主体权利的保护和对数据安全风险的防范,数据保护影响评估(data protection impact assessment,以下简称DPIA)程序应运而生。2021年8月20日通过的《中华人民共和国个人信息保护法》将DPIA定义为个人数据处理的事前数据风险评估程序。

从数据治理初期到数据治理深入发展阶段,新技术工具所承载的功能与使命是不同的,需要适应风险环境,作出动态变化。DPIA作为以技术规制技术的事前数据风险评估机制,能够关注新技术工具在不同治理阶段的特定风险。但是,随着数据治理的深入发展,DPIA也面临困境与挑战。如何兼顾数据处理目的实现与权利保护,成为DPIA无法回避的问题。本文旨在通过厘清我国DPIA的制度定位与架构,分析其应用价值和实践困境,提出建构开放型DPIA的具体举措,推动DPIA充分发挥保障数据处理行为合法、保护个人权利实现的功能。

一、我国与欧盟的DPIA制度定位与架构的对比分析

(一)DPIA的制度定位

1. 事前数据风险评估

DPIA缘起于欧盟一般性资料保护规范(general data protection regulation,以下简称GDPR)第35条之规定,是线上侵犯个人数据事前防范的重要制度。依据GDPR第35条第1款的规定,DPIA评估内容是数据处理行为的性质、范围、背景和目的可能给个人数据保护带来的影响。数据处理活动涵盖的各个阶段,从数据采集直至销毁,凡涉及潜在高风险以至于可能对自然人的权利和自由产生显著影响的行为,均构成DPIA的核心评估客体。这一系列行动包括但不限于数据的搜集、归档记录、系统化构建、储存维护、内容调整、检索利用、公开传播、分配流转、实际应用、最终的安全清除或永久删除等环节。[1]DPIA作为第一个被纳入GDPR的风险管理工具,旨在描述和评估数据处理行为,帮助数据控制者遵守法律规定,帮助数据主体防范自身权利遇到的威胁和风险。

2. 数据控制者的自我规制

DPIA的评估主体是数据控制者,其要求数据控制者自我规制数据处理的风险,并根据风险选择相应的保障措施,将有限的审查资源分配给最可能存在问题的数据处理实践。DPIA根据具体场景将风

[投稿日期]2024-04-18
[基金项目]国家社科基金重大项目(编号:19ZDA163)
[作者简介]高润青(1997-),女,河北邢台人,博士研究生,研究方向:数字法治。

险分成高、中、低三层等级,强调数据控制者应当根据其个人数据处理行为的性质、目的、范围、场景,以及影响公民权利之可能性和敏感度等,承担相应责任。

(二)我国 DPIA 与欧盟 DPIA 制度架构的对比分析

出于对数据处理行为目的和方式正当性的关注以及促使数据安全审查由后端向前端推进,我国在个人信息保护法中规定了 DPIA,并对其评估主体、评估对象和评估步骤作出明确要求。根据个人信息保护法的规定,我国 DPIA 的评估主体为数据处理者,评估对象为个人敏感信息、自动化决策、向第三方提供或公开个人数据,以及向境外提供个人数据等对个人有重大影响的数据处理活动。评估步骤包括确定评估对象、数据映射分析、数据安全风险评估、个人影响分析、采取安全保护措施和整理评估报告等六个步骤。基于对目的限定与比例原则的共同遵循,我国 DPIA 与欧盟 DPIA 在评估主体、评估对象和评估步骤方面均有相同之处。但是,在评估主体的设定、评估对象的标准和评估步骤的操作等方面,二者仍有不同之处,具体分析如下。

1. 评估主体与对象的对比分析

从评估主体来看,不同于欧盟 DPIA 对数据控制者与其他处理者的区分,我国的 DPIA 无差别地要求所有数据处理者开展 DPIA,强调数据安全事前风险的预防无死角。从评估对象来看,欧盟的 DPIA 程序侧重于高风险的判断,而我国的评估程序侧重于对个人信息影响的审查,二者在自动化处理个人信息和境外信息传输领域有交叉,且实质上均以保护个人的自由与权利为目标,见表 1。

表 1 我国与欧盟的 DPIA 对比分析

对比维度	我国 DPIA	欧盟 DPIA
评估主体	数据处理者应对个人数据处理活动在事前进行风险评估,并对处理情况进行记录。	数据控制者负责执行 DPIA 程序,并应咨询资料保护专员。如果数据控制者委托其他数据使用者辅助进行信息处理行为,那么数据使用者应该协助数据控制者进行 DPIA 程序。此外,GPDR 第 39 条第 9 款要求数据控制者在不实际影响商业或公共利益保护或信息使用的前提下,应征求数据主体对其数据使用行为的意见。
评估对象	1. 处理敏感的个人数据。 2. 利用个人数据进行自动化决策。 3. 委托处理个人数据、向第三人提供个人数据、公开个人数据。 4. 向境外提供个人数据。 5. 其他对个人有重大影响的个人数据处理活动。	当某种类型的处理——特别是使用新技术的处理,很可能对自然人的权利与自由带来高风险时,在考虑处理的性质、范围、背景与目的后,控制者应当在处理之前评估对数据保护的影响。 1. 自动化处理并进行广泛的画像分析。 2. 大规模处理特殊类别或刑事犯罪数据。 3. 自动化大规模监控公共场所。 4. 欧盟以外的跨境传输。

2. 评估步骤的对比分析

如图 1 所示,从评估步骤来看,我国的 DPIA 与欧盟的 DPIA 大致相同,均具备完整的评估链条。不同的是,我国的 DPIA 更倾向于静态分析,未将评估报告的强制性公开纳入其中。而欧盟的 DPIA 根据风险等级确认其适用规模,保证评估过程合目的、合比例。DPIA 评估的步骤包括剩余风险的整理,更倾向于动态的全链条的评估,评估报告的公开也更具强制性。

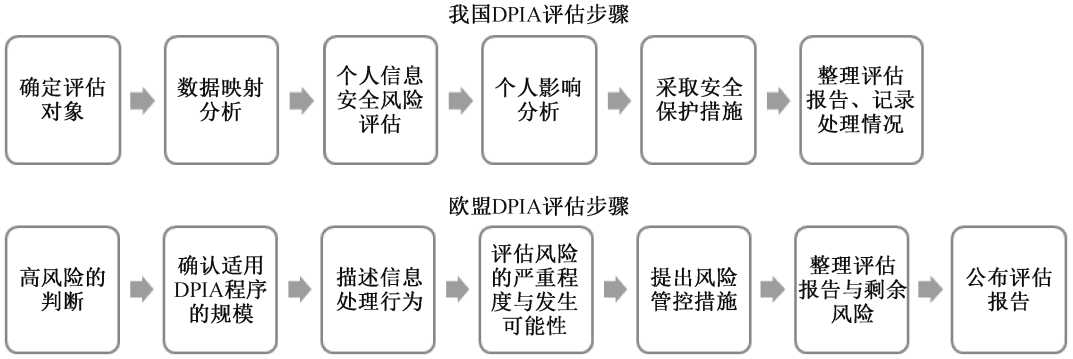

图 1 我国与欧盟的 DPIA 评估步骤

3. 两者共同的关注:目的限制与比例原则

目的限制原则是指收集个人数据时应当明确处理目的,此后的处理活动应限定在该目的范围内。[2] 根据我国个人信息保护法第 6 条之规定,目的限制

包含两方面内容:一是目的明确合理,即要求数据处理者清晰、明确地说明目的,而不是含糊其词、隐晦地表达,同时将目的限定在合法、合理的范围内;二是个人数据处理与初始目的直接相关,即不得逾越初始目的的限定范围,从事无关的处理活动。欧盟要求系统性地大规模监控个体间的接触数据会造成隐私的巨大侵害,原则上需要基于特定目的,最好事先取得信息主体的同意,方可取得处理信息的正当性基础。①

在目的限制明确后,数据处理者仍应注意个人数据的处理符合比例原则的要求。② 我国个人信息保护法明确了个人数据处理行为的必要原则,具体体现为以下三方面的规定:一是处理个人数据应限制在实现处理目的的最小范围内,不得过度收集③;二是个人数据保存期限应为实现处理目的所必要的最短时间④;三是处理敏感个人数据必须具备特定的目的和充分的必要性⑤。此处"实现处理目的的最小范围"应理解为缺少某些特定数据,处理目的就无法完全实现或主要目的无法实现。[2] 与我国对数据处理行为的要求不谋而合,欧盟 GDPR 要求 DPIA 在对接触者追踪程序设计进行评估时,应考虑最少量使用、最短时间存储和最小侵害原则。最少量使用是指程序设计应避免使用可识别的个人数据,不预设数据处理者对所有个人数据如使用者身份、通信识别码、装置识别码、短信、通话记录和地理位置等的掌握。⑥ 最短时间存储要求基于治理目的获取的个人数据在治理任务完成后应被删除或匿名化处理。⑦ 最小侵害原则是指数据处理者可以借助假名化的识别码通知具有关联性的数据主体,但不能试图识别数据主体的具体身份。⑧

二、数据安全风险治理中 DPIA 的应用价值

如上文所述,在数据治理的背景下,DPIA 是数据控制者保证和展示其数据处理行为遵守治理必要性和正当性的方法。DPIA 的功能与我国规制数据治理风险的需求具有相当高的匹配度。我国的 DPIA 在法律规范的指引下已然初具模型,其在数据安全风险治理中的应用价值主要表现为以下三方面。

(一)以事前预防修正事后救济

相较于传统的数据保护模式,DPIA 侧重于事前的风险预防,关注数据处理行为的动态风险管理,并贯穿于规划和执行的全过程,以尽早发现和应对权利风险。[3] 个人数据保护的传统法律框架属于事后救济模式,它只是在个人数据受到侵害时才予以救济。而在大数据时代,数据处理和数据泄露的风险大大增加。即便数据控制者严格履行数据处理原则和行为规范,也难以把控数据处理结果、避免数据泄露的发生。此类风险的存在要求必须在数据处理的全生命周期为其实施动态的风险控制。侧重事前预防和动态预防的 DPIA 能够帮助数据控制者将数据安全风险扼杀在萌芽之中。

DPIA 启动的前提在于高风险存在与否的判断,且在判断时会综合考量数据处理行为的性质、目的、影响范围等要素。DPIA 启动后,基于初期收集的基本数据设定保护目标。该目标涵盖多个维度:不可干涉性、透明度、完整性和机密性,并强调数据的可得性和不可链接性。针对数据处理流程进行模拟分析,旨在发现并评估可能存在的风险及潜在的危害结果,任何目标层面的疏忽均可能导致对数据主体权利的侵犯,形成实质风险。在风险评估阶段,DPIA 不限于对数据控制者行为的审查,还会涉及对其他数据处理者行为的审查。此种目标清晰、结构完整、主体义务明确的事前审查方式能够揭开众多的数据处理者隐匿在大数据背后的面纱。即使数据处理者通过多元数据流通和二次甚至三次转让授权掌控使用者的数字身份,一旦发生数据侵权,司法机关也可以借助 DPIA 在尽可能短的时间内精准确定侵权主体,为数据主体提供及时有效的救济。

(二)以自我规制降低治理成本

数据治理面对的是一个持续生成、多元存储、反复开发利用、广泛跨域应用、涉及众多参与者、跨境流通频繁、采集与处理环节相分离、生命周期短暂且亟须技术创新手段来应对的数据环境。传统的依赖法律制定和执行机构进行全面保护的方式,在技术和经济层面存在显著挑战,并可能带来高昂的治理支出。因此,采用 DPIA 机制,侧重于强化数据控制主体的内在监管职责,这一策略有效地提升了数据

---

①EDPB, supra note 11, para. 24。欧盟数据保护委员会(European Data Protection Board,简称 EDPB)发布的《利用定位数据与接触追踪工具的指引》,下同。

②EDPB,supra note 11,para. 26。

③个人信息保护法第 6 条。

④个人信息保护法第 19 条。

⑤个人信息保护法第 28 条。

⑥EDPB, supra note 11, para. 40。

⑦EDPB, supra note 11, para. 34。

⑧EDPB, supra note 11,para. 47。

治理作业的效能,降低了其实施难度及相关的经济成本,从而激发数据控制者积极探寻并实践自主合规的管理路径。

通过启动 DPIA,数据控制者可以获取数据风险的情境化、合比例判定。我国个人信息保护法平衡个人权利与数据使用利益的立法初衷决定了合比例分析是数据保护必不可少的工具,部分条文也体现出数据保护的目的不是防止对数据主体的任何消极影响,而是防止不合比例的影响。而 DPIA 恰恰可提供动态的、全程的、情境化的、合比例的分析。一方面,DPIA 作为科学的风险评估工具,能够帮助数据控制者判断基于目的、利益的合比例性,决定是否仍继续进行带有部分风险的数据处理。另一方面,DPIA 内含风险与利益平衡的思想,能够帮助数据控制者根据数据主体类别、数据主体规模、时间、行业领域、数据类别等情况判断应选择何种类型的保障措施。

(三)以技术治理补足法律治理

在数据治理的背景下,DPIA 之目的不仅限于技术层面数据风险的评估,还包括法律层面的合规审查。大数据、人工智能等技术的开发与应用具有相当的进阶性,尽管在数据处理方面体现了传统技术无法比拟的优越性,但若被置于一个相对不智能的技术框架下,这类新兴技术也不免存在与实际情况脱节、不兼容的问题。[4]从数据治理初期到数据治理深入发展阶段,新技术工具所承载的功能与使命是不同的,需要适应风险环境,作出动态变化。而 DPIA 在保护法律框架下的强制性义务的同时,具备较强的可扩展性和动态调整能力,[5]能够关注新技术工具在不同治理阶段的特定风险。DPIA 作为以技术规制技术的评估机制,辅助法律制度兼顾治理目的与权利保护。DPIA 通过事前审查收集和使用个人数据的必要性以及个人权利让渡的正当性,能够监督基于治理目的扩张的行政权在法治框架内运行。

DPIA 强调经由对系统、装置或服务的技术设定,实现个人数据保护的法律规范价值,体现了“代码之法”的本质。实践中,技术开发与商业运行往往涉及多个主体,很多运营商选择将技术开发外包给第三方机构。DPIA 不仅要求数据控制者(即系统使用者)承担个人数据保护义务,还要求开发、设计系统的第三方机构同样承担个人数据保护的职责,在系统设计阶段即考虑个人数据保护的需要,将之嵌入系统,通过技术实现规制。DPIA 可以将数据安全风险治理从政策驱动和法律驱动推向设计驱动的新阶段。[6]

三、我国数据安全风险治理中 DPIA 的应用困境

我国立法中规定了 DPIA 程序的基本内容,但其应用前提还有待考察。随着智能科技日新月异的发展,DPIA 在数据安全风险治理中的应用困境也日益显现,主要表现为以下三个方面。

(一)应用场域的泛化可能

DPIA 在数据安全风险治理中的应用并非没有边界。对所有的数据处理行为进行风险评估既无可能也无必要。各个数据处理行为产生的数据安全风险程度并不相同。例如,支付宝的信用评级系统可能涉及个人敏感信息,而网易音乐的推荐算法系统则并不涉及个人敏感信息。不分风险程度地启动 DPIA 必然会导致其应用的泛化。当前,我国存在着多元化的数据保护评估体系,涉及不同法规与管理措施。首先,个人信息保护法要求数据处理者对其行为进行个人信息保护影响评估。其次,工信部针对通信网络企业的相关管理办法中,明确指出了定期实施网络数据安全评估及评测的要求。最后,国家网信办发布的《数据出境安全评估办法》规定,境内数据控制者在向境外传输数据前,需通过省级网信部门向国家网信部门提交数据出境安全评估。这种多样且应用场景各异的规定,易导致 DPIA 应用范围的过度扩大,同时也不利于充分发挥 DPIA 的治理效能。

(二)自我规制的软化倾向

在规制理念上,目前我国的 DPIA 程序更多体现了自我规制理念。DPIA 主要由兼任算法应用者和数据控制者的主体自我主导,并在相对不公开的环境中完成,呈现出自我规制的特征。确保自我规制切实生效的核心要素包括以下方面:行业组织需具有权威性且代表性突出,以驱动自我规制的实施;保障各利益相关者的程序性权益;设立外部参与机制;政府应具有监督职能及执行力,以督管整个自我规制过程的有效运作。[7]依据个人信息保护法的规定,数据控制者在处理个人敏感信息、利用个人信息进行自动化决策等五种个人信息处理活动之前须进行个人信息保护影响评估,不要求事后进行评估,也不要求涵盖算法系统运行的全周期。[8]目前我国的 DPIA 程序缺乏数据主体和有关专家的参与,也未建立强制性披露报告制度,在实践中还呈现出弱强制性和强自愿性的特征,对个人数据保护作用的实现取决于数据处理者的自觉性和主动性,受到“失之于

软”[9]的批判。

新技术工具通过算法决策进入数据治理的公共领域发生行为规范效力,实际上意味着代码成为社会运行规则的一部分,也需要获得公民的认可与服从,才能发挥其规范效力。在数据治理的背景下进行 DPIA,一方面在于以合规审查保护公民的个人数据,另一方面就在于提升公民对数据处理行为的信任度。以自我规制理念为指引,数据处理者在 DPIA 过程中既是运动员也是裁判员。不可否认的是,尽管数据处理者具有专业的技术能力,但是其被待规制利益俘获的风险相当大。这一弊端势必会削弱公民对 DPIA 程序和数据处理行为的信赖,使得数据主体难以产生源于内心的自愿服从,甚至会加重数据主体对个人数据让渡合法性与合理性的疑虑,阻碍数据治理目的的实现。“信任是令任何与人有关的事物枝繁叶茂的温室……一个充满不信任的社会容易被瓦解。”[10]若失去信任的基础,数据治理即使获得强制性力量,也无法获得有序的良性运行。

(三)事前预防与事后归责的失联

在数据安全风险治理中,DPIA 作为一种事前预防手段,仅仅是通往数据处理可知的桥梁,其终极目标是建立负责任的数据处理体系。DPIA 尽管在某些场域下发挥着防患于未然的作用,但是在面对日益复杂和精细的人工智能时,其损害防范成本较高,而收效却难以保证。基于 DPIA 在规制力上的不足,完备的数据安全风险治理体系需要对其链接事后归责制度。事后归责倾向于从法律后果的角度探寻数据安全风险治理,其最终目标是为遭受权利侵害的信息主体提供救济,以规制算法权力的滥用。

从技术和法律两方面审视,算法系统的规制策略包括两个方面。一是预先阶段,数据管理者需阐述系统目标、任务及流程详情,评估并针对可能出现的安全隐患制订相应预防措施。二是追溯责任阶段,需考量系统实际运作中对个体权益的具体影响,据此作出相应的法律责任界定。技术治理与法律治理互为弥合,事前预防与事后治理本质上也互为辅助。在 DPIA 的应用中,数据控制者能够清楚地描述算法系统的目的、运行情况、运行逻辑以及可能发生的实时变化等,但难以确定风险评估过程对最终法律责任的影响。

四、数据安全风险治理中 DPIA 的完善路径

数字经济时代的数据安全,就是既要确保数据密集流动中数据的保密性、完整性和可用性,也要防范数据大规模聚合和分析引发的安全风险。[11]为了充分发挥 DPIA 的功能,增强 DPIA 的实效性,有必要基于算法系统的自我学习特征,建构具有精准性、参与性和开放性的 DPIA。以 DPIA 的启动、主体参与、步骤运行、报告公布等程序机制为视角,开放型 DPIA 的建构可以从以下四个方面着手。

(一)根据风险程度精确应用场域

根据风险程度确定 DPIA 的应用场域和规模,可以适度减轻数据控制者的审查负担,提高数据安全风险治理的精准度,具体操作如图 2 所示。

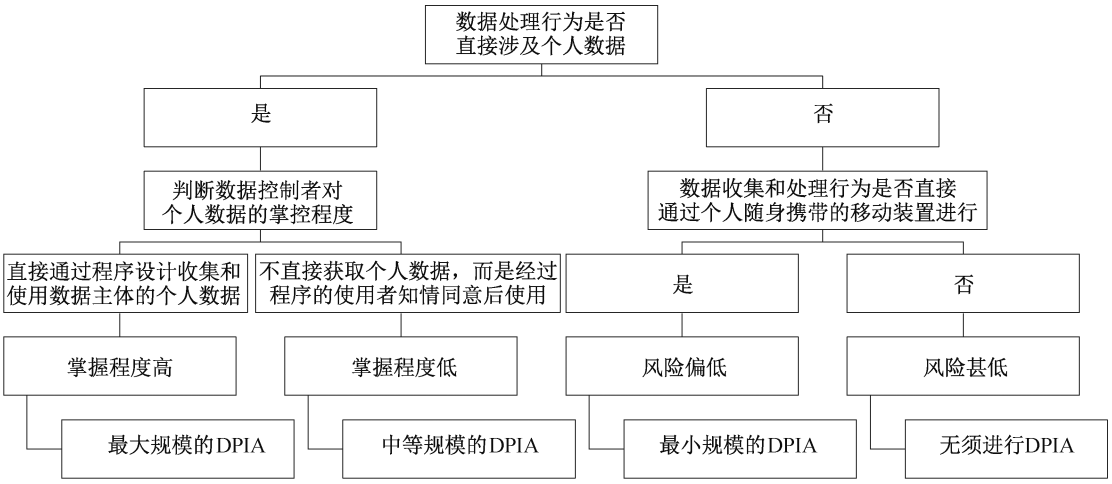

图 2　评估启动 DPIA 程序流程图

(二)保证评估全流程的开放透明

1. 公众风险沟通

基于数据保护影响评估的技术客观性及主观建构特征,借鉴行政领域风险评价实践,主张在数据安全风险管理中,尤其针对存有争议的风险点,应当实施技术民主策略,具体体现为适度公开技术信息并

促进公众参与决策过程。通过集结利益相关者和社会各方力量,对风险进行辨识、理解和合理构建,以推动达成理性的协商共识,这是规避风险的关键举措之一。一方面,数据控制者需要吸纳技术专家的参与,对系统风险进行科学评估;另一方面,数据控制者应在确定评估规模前和形成评估报告前,告知数据主体及其他利益相关者,听取其对评估范围和评估报告的意见建议,使得评估流程更具透明性、评估报告更具合理性。

2. 评估报告强制披露

适当的算法透明具有兼顾公众知情权和市场主体技术创新性的积极意义。[12] 由于评估报告中的内容会对个体权利的保护产生重要影响,数据控制者原则上应公布评估报告的全部内容,涉及国家秘密和商业的内容不予公布,涉及商业秘密的可以作遮掩处理。同时,为保证公众能够充分知悉和了解评估结果,数据控制者在表述方式和公布方式上应使用便于公众理解和获取的方式。

(三)构建内外兼容的协同治理

1. 设立事先咨询机制

在实施 DPIA 过程中,若评估结果显示数据控制者无法有效降低潜在高风险,则需在处理数据之前征询监管机构意见。一旦监管机构判定数据处理活动可能触及数据保护法规且数据控制者无法明确并降低此类风险,监管机构将出具书面建议。这一事前咨询机制的存在,旨在借助政府规制力量,从全局而非个别主体角度,对风险收益与成本进行综合权衡,实现社会整体风险的有效配置及规制效率的最大化。以商业集团开发的医疗诊断软件为例,政府会从社会层面平衡数据处理风险、个人利益和医疗供给问题,而这往往是私人主体难以实现的。此为元规制模式,即政府保持远距离观察,激励数据控制者本身针对问题作出内部式的、自我规制性质的回应。[13]

2. 增设内部制衡机制

目前,在数据控制者内部设立独立的数据保护专员已成为欧美各国 DPIA 实践中的默认规则。数据保护专员是协助和监督数据控制者的数据处理行为,沟通利益相关者(如监管机构、数据主体、商业集团)的有效制度设计。[14] 这一机制有助于促进行业集体责任,打通参与者和利益相关者的整个链条,有助于协调评估标准的制定和分享最佳的实践方式。在设立 DPIA 监管机构的基础上,我国可以通过此机构向数据控制者委派数据保护专员作为数据控制者与数据主体及监管机构间的沟通桥梁,负责 DPIA 的建议、日常数据处理行为的交流以及出现数据保护问题后的咨询。

(四)加强事前预防与事后归责的衔接

1. 根据风险场景认定责任主体

在算法监管的视角下,算法相关方应承担相应责任,即当算法系统实际运作中诱发风险或酿成损失时,无论数据主体事前是否同意或问题起因是否源于技术瑕疵,涉事各方如数据侵害实施者、系统研发者及系统执行者均需承担侵权责任。首先,依据对数据安全隐患对数据主体潜在影响的初步评估来判定侵权责任的可能性,继而通过考察风险情境与现行法规对接来细化侵权责任归属。尽管目前我国法律尚未明文规定算法系统导致的侵权责任分配机制,但仍可借鉴民法典中关于产品责任的逻辑架构来进行责任划分,参见图 3。在实际追责过程中,受损方能够选择向数据控制者或数据处理者提出索赔;若算法风险系由数据控制者触发,已作出赔偿的数据处理者有权向数据控制者进行追偿,反之同样适用。此外,若第三方过失引发了算法损害事件,那么在先行赔付之后,数据控制者和处理者均有权向第三人追偿损失。

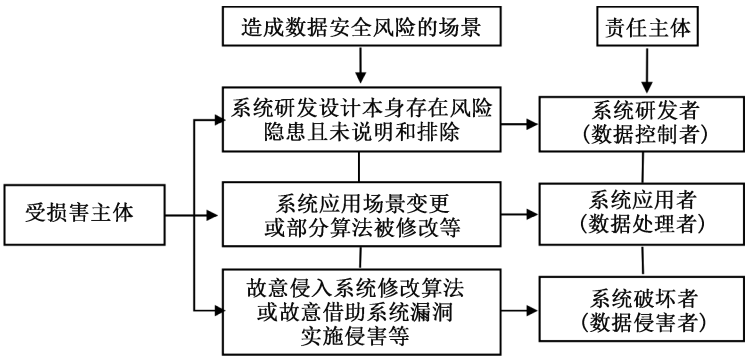

图 3 数据安全风险追责机制图

2. 基于风险路径完善评估链条

如图 4 所示,完善的 DPIA 处置风险流程图包括四个步骤。

第一步是风险源识别,即深入研究数据处理活动所面临的各种威胁源。风险源识别旨在审查现有的安全措施是否足够,以防范系统潜在的风险源和脆弱性,从而避免安全事件的发生。数据安全的风险源既可能来自内部,比如恶意员工或疏忽大意的系统设计参与者;也可能来自外部,如黑客攻击或数据盗窃。此外,脆弱性同样不容忽视,其可能源于物理环境如数据中心的损坏,或是技术层面如数据泄露、篡改和丢失,甚至是管理不善引发的滥用情况。简言之,数据安全的风险源可以概括为四个方面:网络环境和技术措施、数据处理活动、系统设计参与者,以及业务特点和规模。

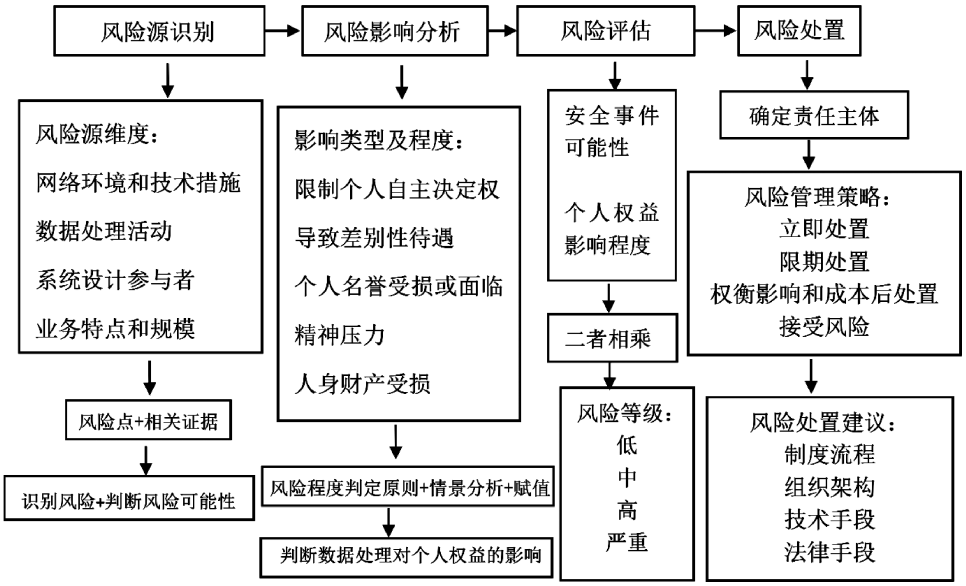

图 4　DPIA 风险处置流程图

第二步是风险影响分析。通过使用专业的风险影响分析工具,数据控制者可以对特定的数据处理活动进行深入的剖析。这些工具通常基于自动化赋值系统进行风险计算,从而得出风险影响指标。风险影响分析主要关注四个维度:是否限制了个人自主决定权、是否导致差别性待遇、个人名誉是否受损或面临精神压力,以及人身和财产是否遭受损失。通过全面考虑这些因素,数据控制者能够更准确地评估数据处理活动对个人数据主体合法权益的影响。

第三步是风险评估。在此环节,数据控制者结合之前的风险影响分析结果,综合考虑安全事件的可能性及对个人权益的影响程度,分析并确定数据处理活动的安全风险等级,进而提出相应的整改措施。

第四步是风险处置。根据安全风险的等级,数据控制者可以采取相应的处置方式,如立即处置、限期处置、在权衡影响和成本后进行处置,或是接受风险。

此外,数据控制者还需持续跟踪风险处置的落实情况,评估剩余风险,确保风险始终控制在可接受的范围内。

五、结语

面对大数据时代下数据处理行为对个体和社会的异化,DPIA 的建构与完善是动态保护个人数据权、保障社会治理目的实现的最新回应。与数据泄露通知的事后介入不同,DPIA 始于数据收集之时,贯穿于数据处理活动的全过程。与外部监管不同,DPIA 是数据控制者对自身的信息处理行为加以检视,约束其自行裁量空间的行为。在数据控制者实现自我规制的基础上,我国未来应向建构开放型 DPIA 的目标迈进。开放型 DPIA 更加透明公开,要求数据控制者根据数据处理行为的风险程度确定评估规模,对数据处理行为的安全性、公平性和权利影响作出评估。在评估阶段引入信息主体和专家参与,设置独立监管机构和数据保护专员,在评估完成后公布数据保护影响评估报告,根据风险等级和角色分工认定责任。建构开放型 DPIA 不仅有助于数据控制者实现自我规制,也有助于数据主体保护个体权利,政府部门防范治理风险,实现大数据时代下数据的共治共享。

参考文献

[1]盛小平,郭道胜.科学数据开放共享中的数据安全治理研究[J].图书情报工作,2020,64(22):25-36.

[2]程啸.论我国个人信息保护法的基本原则[J].国家检察官学院学报,2021,29(5):3-20.

[3]Article 29 Data Protection Working Party. Statement on the role of a risk based approach in data protection legal frameworks[EB/OL].(2014-05-30)[2024-02-14]. https://ec.europa.eu/justice/article-29/documentation/opinionrecommenda-tion/files/2014/wp218_en.pdf.

[4]胡凌.刷脸:身份制度、个人信息与法律规制[J].法学家,2021,(2):41-55.

[5]崔聪聪,许智鑫.数据保护影响评估制度:欧盟立法与中国方案[J].图书情报工作,2020,64(5):41-49.

[6]KLITOU D, Privacy by design and privacy-invading technologies: Safeguarding privacy, liberty and security in the 21st century[J]. Legisprudence, 2011,5(3): 297-329.

[7]李洪雷.论互联网的规制体制——在政府规制与自我规制之间[J].环球法律评论,2014,36(1):118-133.

[8]张恩典.算法影响评估制度的反思与建构[J].电子政务,2021,(11):57-68.

[9]张凌寒.算法评估制度如何在平台问责中发挥作用[J].上海政法学院学报(法治论丛),2021,36(3):45-57.

[10]布鲁斯·施奈尔.我们的信任[M].徐小天,译.北京:机械工业出版社,2013:7.

[11]刘金瑞.数据安全范式革新及其立法展开[J].环球法律评论,2021,43(1):5-21.

[12]崔冬,夏玉配.算法透明的困境及规制路径研究[J].河北工程大学学报(社会科学版),2024,41(1):73-81.

[13]鲍德温,凯夫,洛奇.牛津规制手册[M].宋华琳,李鸽,安永康,等,译,上海:上海三联书店,2019:150.

[14]Article 29 Data Protection Working Party. Guidelines on data protection officers [EB/OL].(2017-04-05)[2024-02-14].http://ec.europa.eu/newsroom/article29/item-detail.cfm? item_id=612048.

[责任编辑 李 新]

The Application and Improvement of DPIA in Data Security Risk Governance in China

GAO Runqing

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

Abstract: In data security risk governance, the DPIA program is positioned as a self-regulator of pre data risk assessment and data controllers. China has stipulated DPIA in the Personal Information Protection Law, and its application value in data security risk governance is reflected in prevention, amendment and post-relief, self-regulation to reduce governance costs and technical governance to supplement legal governance. Faced with the rapid development of intelligent technology, the application dilemma of DPIA in data security risk governance is also increasingly apparent, which is manifested in three aspects: the generalization possibility of application field, the softening tendency of self-regulation and the prevention and post-fault imputation. In view of this, from the perspective of constructing an open DPIA program, this paper puts forward four measures: accurately applying the field according to the degree of risk, ensuring the openness and transparency of the whole process of evaluation, constructing internal and external compatible collaborative governance, and linking prevention in advance and accountability after the event.

Key Words: data security; DPIA program; risk governance