·数字经济·

欧盟数据保护影响评估制度及其镜鉴

□肖君拥　张雪亭
[北京理工大学　北京　100081]

[摘　要]　【目的/意义】欧盟《通用数据保护条例》（GDPR) 创设的数据保护影响评估(DPIA) 制度对数据风险防控具有重要意义。借鉴欧盟DPIA制度可以助益于我国企业数据合规、重要数据的保护、数据安全风险评估标准的构建。【设计/方法】首先，通过梳理DPIA制度的演化背景、理论基础，全面剖析欧盟DPIA制度的应用场景、评估流程、保护模式及惩罚机制。其次，通过梳理相关案例，对事实层面和规范层面我国建立数据影响评估制度的必要性进行分析。再次，对比我国个人信息安全影响评估（PISIA）制度与欧盟DPIA制度在适用阶段、评估目标、评估产物等相关规定的异同，可知前者侧重于对个人信息数据泄露后会对数据主体的影响维度进行分析，后者侧重于对数据主体权益保障维度的分析。最后，以问题为导向，对我国数据保护影响评估制度的建立提出相关建议。【结论/发现】完善数据安全风险评估标准的研制、提升数据安全风险评估质效、构建全方位的数据监管体系，不仅是构建法治化的数据安全风险评估制度的需要，更是我国经济实现数字化转型、构建数据安全保障治理体系的迫切需求。

[关键词]　欧盟数据保护影响评估(DPIA)制度；个人信息安全影响评估(PISIA)制度；数据安全风险评估；数据安全
[中图分类号] D901　　[文献标识码] A　　[DOI] 10.14071/j.1008-8105(2022)-4005

On EU's Data Protection Impact Assessment System and Its Reference to China

XIAO Jun-yong　ZHANG Xue-ting
(Beijing Institute of Technology　Beijing　100081　China)

Abstract　[Purpose/Significance] The Data Protection Impact Assessment (DPIA) system created by the EU General Data Protection Regulation (GDPR) is of great significance to data risk prevention and control. Learning from the EU's DPIA system can help China's enterprise data compliance, the protection of important data, and the construction of data security risk assessment standards. [Design/Methodology] Firstly, by sorting out the evolution background and theoretical foundation of DPIA system, we comprehensively analyze the application scenario, assessment process, protection model and punishment mechanism of EU DPIA system. Secondly, by sorting out relevant cases, the necessity of establishing data impact assessment system in China at the factual level and normative level is analyzed. Then, comparing the similarities and differences between China's personal information security impact assessment (PISIA) system and the EU DPIA system in terms of application stages, assessment objectives, assessment products and other relevant regulations, it can be seen that the former focuses on the analysis of the impact dimension of data subjects that will be affected by personal information data leakage, while the latter

[收稿日期]　2022 – 06 – 06
[基金项目]　教育部人文社科基地重大项目（21JJD820009）.
[作者简介]　肖君拥（1974– ）男，北京理工大学法学院教授、博士生导师，智能科技法律风险防控工信部重点实验室研究员；张雪亭（1997– ）女，北京理工大学法学院硕士研究生，智能科技法律风险防控工信部重点实验室研究助理.

focuses on the analysis of the dimension of data subjects' rights and interests protection. Finally, with a problem-oriented approach, relevant suggestions are made for the establishment of the data protection impact assessment system in China. [Conclusions/Findings] Improving the development of data security risk assessment standards, enhancing the quality and effectiveness of data security risk assessment, and building a comprehensive data supervision system are not only necessary for building a rule-of-law data security risk assessment system, but also an urgent need for China's economy to realize digital transformation and build a data security guarantee governance system.

Key words　EU's Data Protection Impact Assessment (DPIA) system; Personal Information Security Impact Assessment (PISIA) system; data security risk assessment; data security

引言

数字化为促进经济发展提供了新的机会，但也增加了数据主体潜在的数据泄露风险。为帮助数据控制者或处理者评估其数据处理的必要性和适当性，欧盟《通用数据保护条例》（以下简称“GDPR”）在隐私影响评估（Privacy Impact Assessment，以下简称“PIA”）的基础上专门创设了数据影响评估（Data Protection Impact Assessment，以下简称“DPIA”）制度。DPIA制度作为欧盟数据保护框架中的核心内容，不仅成为了各国个人数据安全治理的重要手段，而且为各国企业合规管理、经济数字化转型以及数据安全治理法律体系的构建提供了理想范本。据检索，欧盟学术界目前仅有David Wright、Clarke Roger、F. Bieker等少数几位学者对隐私影响评估(PIA)制度的必要性以及相关学理进行了初步阐述，而国内的相关研究仅停留在泛泛而谈DPIA制度的演化背景、DPIA制度的理论基础，相关研究还不够深入细致。

欧盟GDPR框架下创设的DPIA制度，是否是给欧盟境内外企业增加的又一项新的合规义务？落实DPIA制度仅是为了指引、强制企业遵守GDPR数据合规的相关规定？何种场景下企业应当进行DPIA？如何开展DPIA的具体流程？本文聚焦于对欧盟的DPIA制度的演化、应用场景及评估流程等全方位的介绍、分析与评论，佐以相关实践案例说明落实数据安全风险评估制度的重要性。希望能为我国企业数据合规的思路转换、数据安全保障、数字经济的转型以及构建具有中国特色的数据治理体系提供参考。

一、欧盟数据保护影响评估（DPIA）制度的起源与特点

（一）DPIA制度的源起：从PIA制度到DPIA制度

西方社会的隐私意识觉醒较早，对于隐私问题的较普遍关注，可以追溯到20世纪60年代末的欧洲的公平信息实践（fair information practices，FIPs）运动[1]。为了提高公民福利水平，政府开始利用电子数据库搜集和存储大量的公民个人信息。FIPs运动的最初目的是确保“企业和政府在进行经济活动时，信息技术之手不会导致对隐私的过度侵犯”[2]。FIPs运动在最初期关注的是组织的信息安全，随着对隐私问题认识的深入，人们关注的焦点才逐渐转向个体隐私。FIPs运动成为人们开始关注个体隐私问题的导火索，由此确立的FIPs原则（即FIPP）也成为《OECD隐私指南》《APEC隐私框架》和“ISO/IEC 29100：2011《信息技术安全技术隐私框架》”《美国隐私法案》等后续世界各国（地区）的隐私保护立法的重要准则。

尽管西方社会层面有隐私意识觉醒，但各国政府并未在立法层面给予及时回应。直到20世纪90年代，随着信息时代的到来，隐私泄露风险的遽增，隐私影响评估制度才应运而生并逐渐成为一种保护个体隐私的常规手段。

欧洲议会和欧盟理事会于1995年10月24日通过了《关于涉及个人数据处理的个人保护以及此类数据自由流通的第95/46/EC/号指令》（EU Data Protection Directive 95/46/EC，以下简称《95指令》）。该指令要求各成员国保护自然人各项基本权利和自由，尤其是加强与个人数据相关的隐私权的保护。《95指令》第20条要求信息系统需要通过“预先校验（prior checking）”以验证应用标准的符合性，即要求商业机构收集个人信息必须事先获得个人的明确同意。为适应《95指令》，英国在1998年出台了《数据保护法》，其中规定事先审查这一合规性审查方式，该制度使得英国成为最早实施 PIA 制度的国家。2017年，国际标准化组织发布的ISO/IEC 29134：2017成为PIA最具代表性的标准之一。其将PIA定义为：在组织更广泛的风险管理框架内进行的识别、分析、评估、咨询、沟通和计划处置与个人身份信息处理相关的潜在隐私影响的

整个过程，还对PIA的评估过程、评估报告的结构和内容做了详细的规定[3]。

大数据时代背景下，为进一步保护数据主体的权利和自由，2009年，欧盟委员会启动对《95指令》的修订。2012年，欧盟委员会出台了替代《95指令》的欧盟《通用数据保护条例》（GDPR）草案。2016年，GDPR经欧盟委员会投票通过，并于2018 年 5月25日生效。GDPR强化了数据主体的各项权利，同时对义务主体提出了更严格的要求，加重了后者的数据保护义务和责任。GDPR中增加了数据控制者或处理者的多项义务，其中旨在通过评估数据处理行为的必要性和适当性，并通过评估内容帮助企业最小化个人数据处理活动风险的数据保护影响评估（DPIA）制度，在全球范围内引起了广泛关注。

（二）欧盟DPIA制度的特点

欧盟GDPR中没有正式周详定义DPIA制度。GDPR仅在第35条第（1）款规定：当某种类型的处理——特别是使用新技术进行的处理——很可能会对自然人的权利与自由带来高风险时，在考虑了处理的性质、范围、语境与目的后，控制者应当在处理之前评估计划的处理进程对个人数据保护的影响。若多项高风险处理活动属于同一种类，那么此时仅对其中某一项活动进行评估即可①。即DPIA旨在成为一种灵活的、能够帮助数据控制者或处理者分析、识别和最小化数据保护风险的事前审查工具，或者可以说DPIA是建立和证明数据控制者或处理者数据处理合规的过程，它能帮助管理数据控制者或处理者处理个人数据对自然人权利和自由造成的风险。欧盟DPIA制度有以下三方面特点：

第一，规制对象的变化。需要注意的是，作为PIA制度的延伸，DPIA的规制对象不再是“个人隐私”，规制主体变成了“个人数据”。GDPR第4条规定：“个人数据”是指与已识别或可识别的自然人（“数据主体”）相关的任何信息①。“数据”作为接近事实的最小单元，作为网络中由各种设备存储、传输的各类信息的载体，其范围要远远大于隐私。由此可见，与以往的隐私规则相比，GDPR对“个人数据”的范围进行定义，相较于PIA的规制对象“个人隐私”来说有所扩大。GDPR对获取和管理数据的一整条数据供应链自上而下都提出了更为严格的要求，并赋予数据主体明确的权利，为强化个人数据安全和保护迈出了重要的一步。

第二，法律义务的强化。GDPR第35条第1款对数据控制者或处理者执行DPIA这里用的是“应当”而不是“可以”，当其数据处理行为有可能对数据主体的数据权利和自由带来高风险时，数据控制者或处理者必须进行事前评估。也就是说，DPIA不再像PIA一样仅仅作为一项商业风险防控的手段或监管部门的建议，而是上升为数据控制者或处理者的一项强制性法定义务。

第三，加强问责的合规导向。尽管DPIA仅仅能够帮助数据控制者或处理者最小化风险，不能帮助数据控制者或处理者消除风险，且DPIA是在GDPR下履行问责义务的关键部分，但DPIA不应当仅仅被视为一种加重数据控制者或处理者义务的工具。在Facebook深陷“剑桥分析”数据泄密丑闻事件，认罚50亿美元与美国联邦贸易委员会达成和解后，Facebook首席产品隐私官米歇尔•普罗蒂（Michel Protti）在公司官方博客中写道：“这项协议已经给我们公司带来了根本性的变化，在保护用户隐私方面，我们取得了前所未有的进步。更重要的是，它带来了一种新的问责制，同时确保隐私问题成为了Facebook每位员工所肩负的责任。”[4]可见，施行DPIA制度，可以倒逼企业内部数据合规制度的完善。数据控制者或处理者可以根据其数据处理过程的特点，开发符合自身特点的DPIA模板和流程。尽管DPIA模板和流程的设计不是一次性的练习，需要定期审核、持续更新以及动态监管，但数据控制者或处理者如果将DPIA制度落实到位，不仅可以帮助企业证明合规性，甚至可以为企业带来良好的社会声誉进而为其带来其所期待的商业利益。

二、欧盟数据保护影响评估（DPIA）制度的启动与要求

（一）数据控制者或处理者启动DPIA的场景

通过上文对GDPR第35条第（1）款分析可知，并非数据控制者或处理者的每个数据处理操作都需要执行DPIA，只有涉及高风险数据处理过程时，数据控制者或处理者才需要进行事前评估。那么究竟什么是高风险数据处理过程呢？由表1可以看出DPIA风险评价的两个维度，纵坐标是影响层面的维度，横坐标是风险交叉可能性的维度，二者交叉便可得出是否构成高风险的综合结论。GDPR对于何为数据控制者或处理者的“高风险”活动，并未采取传统的下定义的方式，而是列举了尤其需要进行DPIA的三种高风险典型场景。

表 1　欧盟DPIA制度风险评价维度

		风险等级				
影响	非常高（5）	6	7	8	9	10
	高（4）	5	6	7	8	9
	中等（3）	4	5	6	7	8
	低（2）	3	4	5	6	7
	非常低（1）	2	3	4	5	6
		几乎不可能（1）	可能性极小（2）	可能性较小（3）	可能（4）	几乎确定（5）
		可能性				

GDPR第35条第（3）款规定了需要进行事前评估的三种情形：（1）对自然人进行系统性和广泛性的个人情况评估，且该评估基于自动化处理（包括数据画像）并且基于该评估作出对该自然人产生法律效力或类似重要影响的决定；（2）大规模处理本条例第9条第1款规定的特定类型的数据，或者第10条规定的有关刑事定罪和犯罪的个人数据；（3）对公共区域的大规模系统性监控[①]。

此外关于何种场景下需要进行DPIA，GDPR还从正反两个方面进行规制，第35条第（4）款规定，监管机构应建立一份欧盟通用的需要强制执行DPIA的处理操作清单。需要DPIA的数据处理如：银行根据信用参考数据库对其客户进行筛选；一家医院即将实施一个新的健康信息数据库，其中包含患者的健康数据；公交运营商即将实施车载摄像头，以监控驾驶员和乘客的行为。第35条第（5）款规定，监管机构还应当建立一份不需要进行DPIA操作的欧盟通用公开性的列表。例如：社区医生处理患者的个人数据不需要DPIA，因为社区医生处理的患者数量不是大规模的。当数据控制者或处理者不确定是否需要进行DPIA时，GDPR第35条第（2）款和第36条第（1）款共同规定了数据控制者或处理者应当向数据保护官咨询以及数据控制者或处理者何时事前咨询监管机构的标准。

由此可见，监管机构不仅要建立需要进行DPIA义务的清单，还要制定无需进行DPIA的清单。只有数据控制者或处理者的行为满足了主管部门规定的正面清单要求，才能够被豁免不需履行DPIA义务，否则数据处理行为均需要执行DPIA方法。尽管GDPR竭尽全力从正反两方面描述了需要进行DPIA和不需进行DPIA的情形，且建立了一系列具体的清单，但相较于数据控制者或处理者纷繁复杂的数据处理过程来说，DPIA在具体适用过程中的规定仍然较为模糊和有限，企业在实际数据处理过程中究竟何时需要进行DPIA在法律框架内仍需结合监管机构和数据保护官的意见。

（二）数据控制者或处理者实施DPIA的基本要求

欧盟GDPR框架数据控制者或处理者主动执行DPIA的基本流程主要包含以下四个步骤（见图1）：（1）对是否可能造成高风险的判断；（2）对是否适用于例外情形的判断；（3）执行 DPIA方法；（4）对剩余风险是否仍然高的判断，而后数据控制者或处理者再决定是否执行DPIA。

首先，在进行DPIA之前，数据控制者或处理者应当充分考虑其数据处理行为是否属于GDPR第

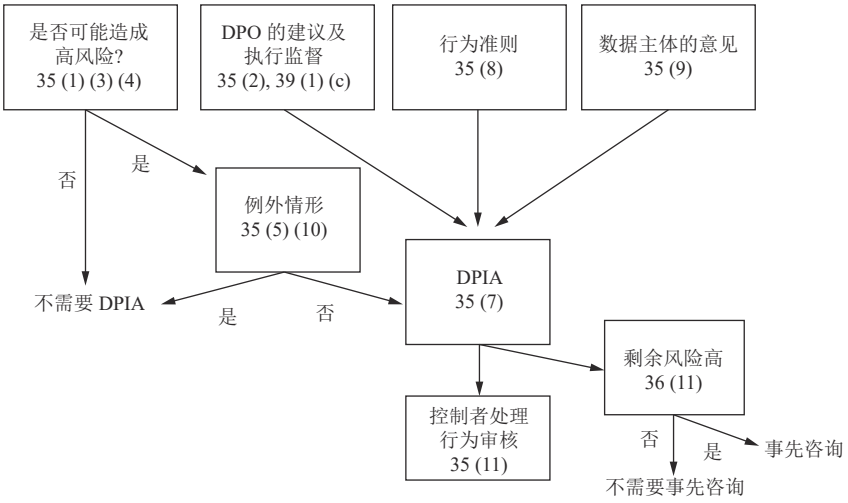

图 1　DPIA 制度的基本流程

35条第（1）（3）（4）款所提到的高风险行为。若数据处理过程不涉及高风险行为，则无需进行DPIA。即便属于高风险行为，若数据处理过程被列入GDPR第35条第（5）（10）款中监管机构制定的无需进行DPIA清单，数据控制者或处理者也无需进行DPIA。这种情况的前提是数据处理过程严格在清单所提及的程序范围内，且继续数据处理过程应完全符合GDPR的所有相关要求。

其次，若存在以下三种情形，也应当进行DPIA：（1）数据保护官及监管机构认为数据处理过程需要进行DPIA时，且数据控制者或处理者应当将相关建议如实记录在DPIA中；（2）数据控制者或处理者在进行DPIA时，应当合理考虑其对第40条所规定的已生效的行为准则的遵守，比如已经生效的欧盟成员国、行业协会等机构制定的行为准则等；（3）在不影响商业利益公共利益、数据处理操作的安全性的前提下，数据主体预期数据处理进行DPIA时，应当充分考虑、咨询数据主体对于数据处理的观点，如果数据控制者或处理者的最终决定与数据主体的观点不同，则应记录其进行或不进行DPIA的原因。

最后，执行DPIA并不是一劳永逸的，而是一个动态监管的过程。为了管理关于自然人的权利和自由的风险，在对风险进行一次识别、分析、评估、处理后还应当进行定期审查。数据控制者或处理者并不能以已经执行DPIA来抗辩其数据保护义务和责任。因此，若进行DPIA后仍显示出较高的剩余风险，如数据控制者或处理者涉及数据的共享、数据跨境传输或软件更新后，他们可能进行DPIA后仍会显示高风险。此时数据控制者或处理者需要咨询监管机构。在数据控制者或处理者提供DPIA后，监管机构应在规定限期内向其提供书面建议。

三、欧盟建构DPIA制度的实践与动因解析

（一）基于企业合规的需要

DPIA制度堪称一项保障企业数据合规的工具。企业向数据主体展示数据控制者或处理者的责任制度，甚至向数据主体公开DPIA模板，有利于获取数据主体的信任。试举两例如下：

Knuddels.de是德国的一家社交平台。2018年，因未采取任何保障措施，80万封电子邮件地址和180多万个用户名和密码被黑客以明文形式公布在互联网上。Knuddels.de平台在处理大量用户数据前，未进行数据保护影响评估，德国数据保护当局决定对其处2万欧元的罚款[5]。

2020年芬兰数据保护申诉专员办公室对违规处理员工位置数据的开曼•韦西公司处以16 000欧元的罚款。该公司使用车辆信息系统跟踪车辆来分析其员工的位置数据，且在处理之前未进行DPIA，其数据处理过程涉嫌侵犯员工隐私[6]。根据不同的违规使用数据行为，GDPR第83条定义了两类处罚标准，第一等级最高可处以1 000万欧元，或上一财年全球营业额2%的行政处罚，以较高者为准；第二等级最高可处以2 000万欧元，或上一财年全球营业额4%的行政处罚，以较高者为准①。

可见，数据处理过程中若企业需要进行DPIA时未履行相关义务，可能会因违反GDPR而面临十分严厉的执法处罚。可以说，进行DPIA并发布数据评估报告是证明企业遵守了GDPR的一种广泛性合规手段。因此，对可能个人数据造成高风险的数据处理过程开展DPIA，不仅能够降低对数据主体合法权益的不利影响，而且出于审慎经营的目的，执行DPIA能够为企业的声誉维护和品牌建设等带来更为广泛的利益。

（二）基于人权保护的需要

进行DPIA不仅是基于企业合规的要求，更是保障特殊群体人权的重要措施。2018年7月17日，葡萄牙数据监管机构（CNPD）对违反了“数据最小化原则”的Barreiro医院处以40万欧元的罚款。Barreiro因为将临床数据的访问权限分开，在传送患者医疗数据前未进行DPIA，导致患者临床数据泄露[7]。

2020年，挪威数据保护局对Raelingen市处以47,500欧元的行政罚款。该市市政当局使用了一款名为Showbie的app处理有特殊需要的儿童健康数据，但在应用程序投入使用之前，未尽到数据安全保障义务，导致未被处理的其他儿童的个人数据大面积泄露。早在2018年12月，挪威数据监察局就因卑尔根市违反挪威隐私条例对其处以了17万欧元的处罚。挪威数据监察局认为卑尔根市小学使用的计算机系统中的个人数据安全性不够，导致卑尔根市35 000多名用户（主要是儿童）的用户名和密码文件被泄露。2019年4月29日，挪威数据保护监管机构对奥斯陆市教育局做出200万挪威克朗（约20.3万欧元或153万人民币）处罚决定[8]。

2019年8月20日，瑞典数据检查局对Anderstorps高中处以20万瑞典克朗，约合2万欧元的罚款。尽

管Anderstorps高中在处理学生人脸识别信息时已经征得了其监护人的同意，但依旧有导致学生出勤信息被泄露的风险。学校的数据处理行为既未进行事前评估，也没有事先咨询瑞典数据保护机构。因此，瑞典数据检查局认为，学校不能以监护人事前同意作为其数据处理行为合法性的基础[9]。

综上，对待特殊主体的数据尤其是弱势群体如儿童数据、健康医疗数据的安全，欧洲国家的监管当局的态度相当严厉。数据控制者或处理者在对弱势群体的相关数据进行处理前应当格外谨慎，包括但不限于实施对数据进行DPIA、匿名化处理、通过区块链等技术对共享数据进行保护、定期测试和评估处理过程的有效性等措施，以防止重大安全漏洞。

（三）基于经济高质量发展的需要

2022年4月21日，美国商务部宣布将成立全球跨境隐私规则论坛（CBPR）。CBPR宣言声明建立的论坛“以促进互操作性”，并“在数据保护和隐私的不同监管方法之间架起桥梁”。目标包括基于亚太经合组织CBPR和PRP系统的认证体系，定期审查成员的数据保护和隐私标准，以及促进与其他数据保护和隐私框架的互操作性。根据其运营目标，论坛成员将进行磋商和交换意见，并分享研究、分析和政策想法。宣言指出，参与“原则上旨在向那些接受论坛目标的司法管辖区开放”，成员共识将决定未来的参与。

可见，全球化经济时代，企业若想走向国际市场，实现长足发展，将世界各国的数据保护规则合规落地是必不可少的环节。如GDPR适用长臂管辖原则，若信息的采集和处理过程均是在欧盟境外完成，则GDPR不适用。但是，如果数据是企业通过提供面向欧盟的服务而在线收集而来的，则受到GDPR的管辖。例如，某App有德语版本，并在德国宣传其可为德国游客在中国的旅行提供服务，则该德国用户的数据需受GDPR管辖。

由此推论，我国外向型涉数字类企业应实行数据保护的思路转换，协调各国数据保护法律的一致性。在处理敏感数据、利用数据进行自动化决策等高风险处理活动时，严格依法落实事前数据安全风险评估制度，对于企业和相关监管部门发现潜在的数据安全风险，具有十分重要的意义。

2021年7月22日，荷兰数据保护局决定对短视频社交平台TikTok（“抖音”国际版）处以75万欧元的罚款。这一事件意味着GDPR实施三年以来，中国企业（包括其控制的海外平台）第一次因违反GDPR相关条款而遭受处罚，具有一定标志性意义[10]。

本案中，罚金之所以为75万欧元，是因为荷兰为执行GDPR而制定了适用本国企业的认定规则《2019年行政处罚管理规则》，相对于GDPR的处罚规定优先适用。如果荷兰没有制定此类处罚管理规则，Tiktok理论上将自动适用GDPR第83条第（4）款的规定，即高达1 000万欧元或前一年全球营业额总额的2%的行政罚款。实际上，欧盟成员国制定这类在本国适用的处罚管理规则并不多见。同时，荷兰对Tiktok进行处罚后，引起了一系列的连锁反应，欧盟其他成员国对Tiktok是否侵害其境内儿童的隐私问题也开始进行调查，所有调查结束后，Tiktok所面临的处罚总额可能更大。

因此，上市公司对可能出现的数据违规行为进行总结，在公布隐私政策时，考虑不同数据主体的特殊性进而进行事前的数据风险评估，加强内部合规管理的制度建设，不仅是企业在海外市场长足发展的重要举措，同时，对我国有效防控市场风险、提高经济发展质量、打造有韧性有活力的资本市场也具有重要而深远的意义。

（四）基于国家安全的需要

2007年Facebook增加了开放应用接口以增加用户App使用时间，用户授权后可对用户的姓名、性别、政治立场等个人信息进行收集。剑桥分析（Cambridge Analytica）是英国一家数据分析公司，其开发了一款针对选民的测试软件，在用户不知情的情况下对政治立场信息进行收集，利用该测试软件，剑桥分析公司获得了用于分析预测用户政治立场的高达 3 000 万份问卷。受雇于特朗普的剑桥分析公司利用Facebook的用户数据，通过客户政治立场的精准画像，进行相关广告投放，对特朗普赢得美国总统大选起到了至关重要的作用。

截至2021年3月31日，作为最大出行平台的滴滴拥有全球年活跃用户近 5 亿，平均日交易量达到4 100 万单，每天新增数据超过108TB。而在赴美上市的审计底稿里，所有数据都是未经过脱敏的原始数据。滴滴的用户数据、会议记录、电子邮件以及政府部门往来的所有机密信息的数量都是其行业中当之无愧的第一名。2021年7月1日，滴滴在官网未发布任何公告、未敲钟的情况下，在美悄悄上市。随即中央网信办以“防范风险扩大”为由对滴滴启动调查程序的深入，滴滴事件一时间引爆舆论[11]。

随着国际环境的日益复杂，实行类似DPIA制度也是贯彻落实总体国家安全观的需要。各国数据

安全保护影响评估制度都强调，DPIA不是一个静态的过程，出具评估报告也不是DPIA的终结，识别和控制风险应当贯穿数据处理过程程序或系统开发生命周期的始终。对于拥有海量数据的企业来说，内部在进行系统更新或数据跨境传输等高风险处理活动前，应当设立DPIA内部审核机制，对后续的数据处理过程持续跟进评估。对于我国相关监管机构来说，加强第三方监督工作力度，对企业数据合规采取包括但不限于DPIA手段在内的更加严格的监管手段，探索出一条大数据时代的企业合规监管路径不仅是建立数据安全治理体系的需要，更是贯彻落实总体国家安全观的必由之路。

四、欧盟DPIA制度与我国PISIA制度的异同

（一）欧盟DPIA制度与我国PISIA制度适用条件的异同

我国在个人信息安全影响评估领域起步较晚，从2017年开始实施的《网络安全法》开始，《数据安全法》《个人信息保护法》以及从民事权利角度强化对个人信息的保护的《民法典》相继出台，呈现出“山顶千门次第开”的景象。

2020年发布的《信息安全技术个人信息安全影响评估指南》（GB/T 39335—2020，以下简称《评估指南》）在充分借鉴了美、欧等国家和地区最新法律规定、制度设计和实践做法后，为《个人信息保护法》的实施提供了坚实且科学的基础。

《网络安全法》在第17条、26条、29条、38条、53条、54条规定开展网络安全风险评估活动，对关键信息基础设施进行，建立健全网络安全风险评估机制，对网络安全风险信息进行分析评估，但仅有模糊性的原则性规定，无具体的实施细则。2017年由全国信息安全标准化技术委员会制定并发布的《信息安全技术个人信息安全规范》（GB/T 35273—2017）（以下简称《规范》）首次提出开展“个人信息安全影响评估”的要求，在信安标委制定的诸多信息安全技术国家标准中，《评估指南》为数据安全影响评估提供了更为具体的方法论和指引。

2021年11月1日起施行的《个人信息保护法》为我国数据保护影响评估制度提供了法律依据。《个人信息保护法》第61条第（4）款规定，推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务，为监管部门执法以及企业合规工作提供了评估原理、实施流程、评估要点以及参考方法。《个人信息保护法》及《评估指南》的出台使我国首次有了较为权威的评估个人信息安全的方法论与路线图。

从二者的主要内容来看（见表2），欧盟DPIA制度侧重于判断是否可能导致自然人权利与自由的高风险，我国PISIA制度则列举了更多评估场景的细分，如《评估指南》中列举了4种场景：（1）业务模式、互联网安全环境、外部环境发生重大变化；（2）发生重大个人信息安全事件；（3）发生收购、兼并、重组等；（4）其他。二者适用情况相似，并具有部分重叠，仅在侧重点方面略有不同。

表 2　欧盟DPIA制度与我国PISIA制度主要内容对比

	GDPR第35条	《个人信息保护法》第55条、第56条
需要进行风险评估的情形	当某种类型的处理——特别是适用新技术进行的处理——很可能会对自然人的权利与自由带来高风险时，在考虑了处理的性质、范围、语境与目的后，控制者应当在处理之前评估计划的处理进程对个人数据保护的影响。若多项高风险处理活动属于同一种类，那么此时仅对其中某一项活动进行评估即可。	利用个人信息进行自动化决策
	以大规模处理的方式处理第9（1）条所规定的特定类型的数据	处理敏感个人信息
	处理与定罪、违法相关的个人数据	委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息
	以大规模的方式系统性地监控某个公众可以访问的空间	向境外提供个人信息
风险评估的内容	对计划的处理操作和处理目的的系统性描述，以及—如果适用的话—对控制者追求的正当利益的描述	其他对个人有重大影响对个人信息处理活动
	对和目的相关的处理操作的必要性与相称性进行分析	对个人权益对影响及安全风险
	对给数据主体对权利与自由带来的风险的评估	

（二）欧盟DPIA制度与我国PISIA制度适用阶段的异同

从二者的适用阶段来看（见表3），我国PISIA制度和欧盟DPIA制度的适宜阶段倾向略有不同。欧盟DPIA制度侧重于个人信息处理活动前以及持续关注风险的态度，来发现随时可能发生潜在对自然人权利和自由带来高度风险的情况。我国PISIA制度其核心思路是从四个可能存在风险或发生安全

表 3　欧盟DPIA制度与我国PISIA制度适用阶段对比

欧盟DPIA制度	中国PISIA制度
1. 事前评估：符合适用条件下，在开展个人信息处理活动前（GDPR第35条第（3）款） 2. 持续评估：未满足触发DPIA义务的条件，并不能降低控制者实施适当管理数据主体权利和自由风险的一般义务：实际上，这意味着控制者必须不断评估其处理活动所产生的风险，以便确定何时进行某种处理“可能对自然人的权利和自由造成高风险” 参考WP29 Guidelines，即欧盟第29条数据保护工作组《数据保护官指南》	1. 事前评估：新产品或新服务设计/上线前 2. 事中评估：业务模式、互联网安全环境、外部环境发生重大变化/发生重大个人信息安全事件后 3. 持续评估、产品或服务整体年度评估 4. 外部因素：法律法规、政策、标准出现重大变化 5. 其他适用情况 参考中国GB/T39335-20205.1.2.2条

事件的维度出发，评估可能对个人权益造成的影响以及风险。

（三）欧盟DPIA制度与我国PISIA制度评估目标的异同

从二者的评估目标来看（见表4），欧盟DPIA制度与我国PISIA制度侧重的适用阶段倾向不同。欧盟DPIA制度侧重于个人信息处理活动前以及持续关注风险的态度来发现随时可能发生潜在对自然人权利和自由带来高度风险的情况。我国PISIA制度根据适用条件，按需进行，包括不限于个人信息处理活动的事前事中定期持续、外部因素变化等情况。

表 4　欧盟DPIA制度与我国PISIA制度评估目标对比

欧盟DPIA制度	PISIA制度
1. 识别处理活动，包括程序、系统、功能、项目和流程中个人数据的特定风险	1. 识别组织的个人信息处理活动的风险并作为合规的证明，减轻事件发生时的责任
2. 作为落实GDPR规定的数据基本处理原则可问责性（Accountability）的基本措施	2. 识别与组织合作的第三方的个人信息安全保护能力
3. 通过评估以确定并减少高风险数据处理活动给个人带来的风险	3. 面向监管机构的监督或调查所需证据准备

（四）欧盟DPIA制度与我国PISIA制度评估步骤对比

从二者的评估步骤来看（见图2），欧盟DPIA制度与我国PISIA制度在评估步骤的流程上大致相同。从评估的发起主体来看，我国PISIA制度分为两种，一种是数据控制者或处理者自行发起对个人信息处理过程的自评估，一种企业等上级组织或监管部门对数据控制者或处理者发起的检查评估。从评估的实施主体来看，企业既可以在内部设置专门的法务或合规部门负责评估，也可以委托第三方专业机构进行评估，如网络安全评估机构、律师事务所等。

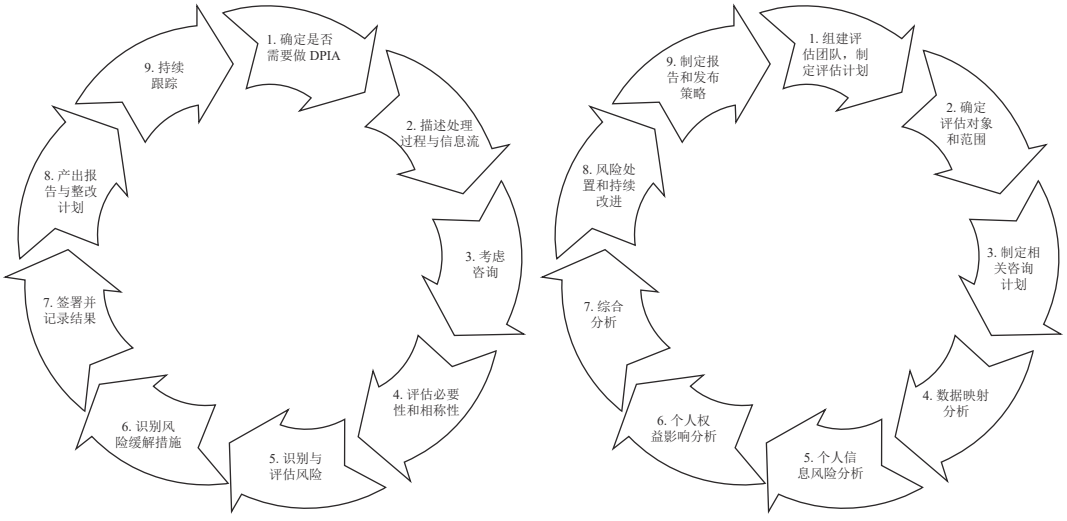

图 2　欧盟DPIA制度与我国PISIA制度评估步骤对比

（五）欧盟DPIA制度与我国PISIA制度评估产物的异同

从二者的评估产物——评估报告来看（见表5），二者的评估报告十分相似甚至有相当部分的重叠，仅在某些细节上略有区别。欧盟DPIA制度中的评估报告对数据主体权益和自由的合规评估更加突出，而我国PISIA制度中均衡了隐私权益和信息安全保护措施，视情况会有实际安全测试、安全审计报告。相比于欧盟的DPIA制度，我国PISIA制度的评估报告的侧重点更加突出“安全”，信息安全要

素权重占比更高。在数据控制者或处理者发生数据安全事件时，尽管出具数据评估报告不能豁免企业的相关责任，但评估报告及其形成报告过程中的相关记录，有助于减轻企业的相关责任和名誉损失，更重要的是有利于进一步查找企业的数据安全风险的漏洞所在。

表 5 欧盟DPIA制度与我国PISIA制度评估报告内容对比

欧盟DPIA制度评估报告内容	我国PISIA制度评估报告内容
1. 处理过程描述及目的说明以及遵守的行为准则 2. 评估合法权益、必要性与相称性 3. 评估数据主体的权利和自由风险及设想的风险应对措施 4. 落实合规安全措施的证明 5. 时间范围策略的规定（如涉及数据删除）及PbD②的规定 6. 个人数据的接收者 7. 是否咨询国数据主体并获得其同意的详细信息	1. 审批页、撰写人、适用范围、评估依据 2. 评估对象、内容、相关方 3. 数据映射分析、个人权益分析、风险分析的过程和结果（包括但不限于访谈、制度、日志配置、安全测试等） 4. 风险判定准则、风险与合规判定结论与处置建议 5. 过程中其他附件

（六）欧盟DPIA制度与我国PISIA制度执行力度的异同

从二者的执行力度来看（见表6），我国PISIA制度的执行力度稍显不足。GDPR第83条定义了两类处罚标准，第一等级最高可处以1 000万欧元，或上一财年全球营业额2%的行政处罚，以较高者为准；第二等级最高可处以2 000万欧元，或上一财年全球营业额4%的行政处罚，以较高者为准①。我国《个人信息保护法》第66条也规定了两类处罚标准，第一种：情节较轻的，由相关部门责令改正，给予警告，没收违法所得，责令暂停或者终止提供服务；拒不改正的，并处100万元以下罚款；对相关责任人处1万元以上10万元以下罚款。第二种：情节严重的，由相关部门责令暂停相关业务、停业整顿或吊销相关许可、营业执照；并处以5 000万元以下或者上一年度营业额5%以下罚款。对相关人员处10万元以上100元以下罚款。《个人信息保护法》第68条规定了监管机构未履行相关责任对惩罚机制，第69条规定了数据控制者或处理者的侵权责任归责原则采用过错推定原则，即个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

表 6 我国《个人信息保护法》相关执法案例

公司名称	行政处罚决定文书号	处罚类别	处罚事由	处罚依据	处罚结果
深圳华秋电子有限公司	深福公（梅林）行罚决字〔2022〕33910号	警告；责令停产停业	非法获取、出售、向他人提供个人信息。	根据《网络安全法》第六十条、六十四条和《个人信息保护法》第六十六条	警告、责令限期改正
深圳市辰瑞文化传播有限公司	深福公（天安）行罚决字〔2022〕33751号	警告	2022年3月28日，省厅网警总队线索通报，发现“深圳市辰瑞文化传播有限公司”旗下应用“花遇”，技术检测分析“花遇”应用存在以下违规行为:1.App 首次运行未经用户阅读同意隐私政策，就开始收集个人信息MAC地址、IMEI、AndroidID和应用列表信息。你单位的行为已构成非法获取、出售、向他人提供个人信息相关规定。	根据《网络安全法》第二十二条、第四十一条和第六十四条，《个人信息保护法》第十三条、第六十六条	决定给予深圳市辰瑞文化传播有限公司警告的行政处罚。根据《公安机关办理行政案件程序规定》第一百六十一条第一款之规定，二项行政处罚合并执行，决定给予警告的处罚。
江苏东风南方汽车销售服务有限公司南京分公司	江决字〔2022〕第06号 2022〕第06号	警告	江苏东风南方汽车销售服务有限公司南京分公司在公共场所安装图像采集未设置显著的提示标识。	《个人信息保护法》第六十六条	根据《个人信息保护法》第六十六条之规定，决定给予警告的处罚
深圳志辰网络科技有限公司	深罗公（黄贝）行罚决字〔2022〕33280号	警告;责令停产停业	深圳志辰网络科技有限公司的APP存在隐患：1. 用户登录账号后无法查阅隐私政策，违反便于查阅原则。2. 未在隐私政策等公示文本中逐一列明APP所集成第三方SDK收集使用个人信息的目的、方式和范围。	根据《网络安全法》第六十四条和《个人信息保护法》第六十六条	决定给予深圳志辰网络科技有限公司警告的行政处罚，并责令限期改正。

案件信息来源：威科先行·法律信息库

仅从法律责任的规定来看，我国《个人信息保护法》通过专章设置了较为严格法律责任，并对违法行为实施分类处罚，为监管执法提供了更为明确的上位法依据。但由于《个人信息保护法》实施时间短，执法层面相对落实不到位的情况仍然普遍存在。

尽管随着《个人信息保护法》《规范》《评估指南》等文件的出台，清晰地表明了我国在整体合规趋势上的立法态度，但通过威科先行•法律信息库对违法《个人信息保护法》的实务案件进行搜索，我们发现相比于欧盟DPIA制度来说，我国相关执法案例仍然较少，且处罚基本以警告为主，责令停产停业为辅，仍存在处罚过轻、执行力度不足等问题。

五、欧盟DPIA制度对我国的镜鉴

（一）聚焦数据安全，加快数据安全风险评估标准的研制

随着数字经济时代的到来，数据作为推动全球经济高质量增长的资源性要素，已经成为国际竞争的战略制高点。21世纪以来，欧美等西方国家都开始着手建立本国的数据安全风险评估标准。习近平总书记认为“数字技术正以新理念、新业态、新模式全面融入人类经济、政治、文化、社会、生态文明建设各领域和全过程，给人类生产生活带来广泛而深刻的影响”。2022年6月22日，中央全面深化改革委员会第二十六次会议审议通过了《关于构建数据基础制度更好发挥数据要素作用的意见》，习近平总书记强调，数据基础制度建设事关国家发展和安全大局，要维护数据安全，保护个人信息和商业秘密，促进数据高效流通使用、赋能实体经济，统筹推进数据产权、流通交易、收益分配、安全治理，加快构建数据基础制度体系[12]。利用大数据技术手段提升国家治理体系和治理能力现代化是大势所趋，统筹数据安全和发展并重，加快数据安全风险评估标准的研制，已经成为构建中国特色数据安全治理体系的必然要求。

我国数据安全行业正处于高速发展期：2018～2021年，国内网络安全市场整体增速约20%～23%，同期数据安全市场增速约30%～35%，是同期网安整体增速的1.5倍以上，可见数据安全市场在网安整体市场中占有举足轻重的地位。2021年数据安全市场规模已达近70亿元，未来3~5年，数据安全市场规模将继续保持继续高速增长态势[13]。尽管我国在法律层面，已有“3法+1条例”作为支撑，但远远不能满足市场需求。

数据并非可靠，伪造数据、数据失真、数据失效不仅会使得数据分析、预测失真，而且会导致数据在传输、使用、共享等过程中引发敏感信息泄露风险。随着企业数据量和复杂性的不断增长，数据的应用具有范围广、场景多、过程复杂等特点，一旦发生数据安全事件后造成的影响不可估量。为进一步应对日益严峻的国内外数据安全形势，适应新形势下新技术、新应用、新业态带来的评估对象范围、方式方法的变化，规范企业数据安全产品互联互通框架、提升数据安全服务能力，加强新技术新应用带来的安全问题的风险防控，因此，加快探索并建立并研制包括数据安全风险评估在内的等一批急需关键标准势在必行。

（二）加强行业自律，建立内外审相结合的数据安全风险评估机制

大数据具有“大量、高速、多样、价值、真实性”即“5V”的特点，区别于传统的单线内、外审操作，推进将原有的单向规制转变为内外审相结合的双向数据安全风险评估，有利于在信息化时代建立执行力度更大、速度更快、纵深和延展性更好的数据安全风险评估制度。从《评估指南》中描述的评估发起主体来看，评估工作既可以由企业专门部门负责也可以由外部专业机构开展。但无论是企业指定的内部责任部门还是外部专业独立第三方机构进行数据安全风险评估工作，我们都应当加强行业自律，应当充分保证该部门及相关人员的独立性，保证实施过程的客观性，以免受到被评估方法的影响而使评估过程流于形式。

此外，GDPR第35条第（1）款规定，“一次评估可能涉及一组具有类似高风险的类似处理操作”①。例如全国铁路运营商可以采用统一的数据安全风险评估流程、全国售楼处可以使用统一的数据安全评析评估流程等，以减少对自然人的肖像权等权利造成高风险的情况发生。构建不同行业数据的制式评估流程相比于企业对单个数据处理流程能够大大提高数据安全风险评估的效率。

在我国尚未研制出数据安全风险评估标准以及建立起基本的数据保护法律体系框架之前，由各省市出台因地制宜的政策，行业协会及头部企业充分发挥其协调、带头作用，探索出针对行业共性问题的解决方案。相关行业协会应带头建立起本行业的大数据审计平台和数据运营管理机制，利用数据湖架构搜集和存储企业内、外部结构化和非结构化数据，对行业数据全生命周期的风险进行事前防控。如针对拥有客户静态资产数据以及动态交易数据最多的银行业，其涉及的业务之多、范围之广、关系之复杂是其他行业无法比拟的，行业协会在保障储户金融数据安全方面具有义不容辞的责任。行业协

会应当带头建立起包括采集、加工、转换、存储、交换、关联、共享和管理的全过程数据安全风险防控机制。

因此，行业协会可以建立本行业的数据处理统一平台（见图3）。此平台应加大人工智能、MySQL、HIVE打标与自动扫描、算法黑箱等流程自动化工具的使用，以实现全面提升数据安全风险评估质效的目标。相关人工智能技术可以帮助人员完成外部数据采集、比对分析、系统安全检查以及数据安全风险评估底稿采编等重复性的事务工作。通过相关技术采用文字识别、人脸识别、语音识别等技术还能够对数据安全风险评估中的海量文本、电子证照、录音等非结构化数据的全样本检查后，形成隐形的数据关系，为人工审核提供了一条基于数据的风险和识别路径。此外，通过对机器学习模型后的结果展开进一步分析，可以扩展原有的行业各类数据模型的范围并提高其数据风险识别精度。加强行业自律、发挥企业的主观能动性。采用国家标准与行业自律相结合的方式，才是我国建立内外审相结合的数据安全风险评估机制的最佳选择。

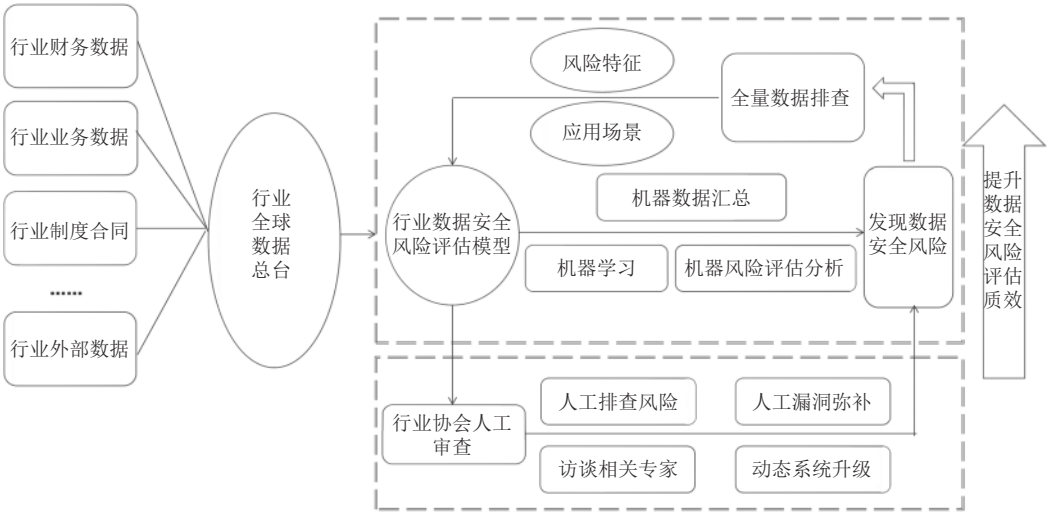

图 3 行业统一平台进行全量风险排查示意图

（三）推进阈值分析，全面推进数据分类分级制度的落地应用

就我国而言，尽管《评估指南》规定了在开展评估前，需要对评估的对象形成清晰的数据清单及数据映射图表，但尚未建立起提高PISIA可操作性的“小规模”数据安全风险评估机制。欧盟DPIA在英国应用时，英国并未将其规定为一项强制性义务，而是用隐私阈值分析（PTA）工具来确定英国进行“全面PIA”还是小规模“PIA”[14]。通过PTA 发现，如果只有一个或两个方面引起隐私问题，那么可以通过小规模 PIA来解决这些问题；如果多个问题的答案是肯定的，则需要全面的 PIA。

DPIA在实践中最大的痛点和难点即在一般的企业场景中，触发DPIA的概率并不算高，但启动DPIA的成本却很高。若对于具体数据评估的必要性存在模糊性和较大的不确定性，就难免存在数据安全风险评估疏漏、实效性差的情况，数据安全风险评估就很有可能陷入被动和低效。因此，我国可以借鉴英国经验，通过 PTA 来记录已经进行数据处理行为，进行阈值分析，推动数据分类分级制度的落地，不仅有利于全面提高数据安全风险评估质效，而且已经成为数字经济时代数据治理的必选题。

通过数据分类对不同数据资产进行编目、标准化，为数据进行确权、管理数据安全风险、责任数据安全落实等提供依据；通过数据分级将数据根据敏感程度和遭到篡改、破坏、泄露或非法利用后对社会的影响程度按照一定的原则和方法进行排序，为数据资产的共享、利用、数据安全风险评估提供依据。实施数据分类分级要以业务为基础，以技术为支撑，利用数据标签技术、知识图谱技术进行系统自动化扫描简化数据分类分级的过程，根据预定参数对数据进行分类分级。数据分类分级制度的落地，将对企业的数据安全风险评估起到指引作用。哪些数据可以使用，哪些不可以使用，哪些能够对外开放，哪些不能对外开放，不同等级的数据在不同场景使用哪种数据安全风险评估策略将一目了然。

数据分类分级不仅是企业安全合规使用数据的基础，更是提升数据安全风险评估质效的良方。最小化数据风险和提升数据安全风险评估质效之间采取保持一种复杂而微妙的动态平衡，兼顾效率和公

平，是推动我国数据安全风险评估机制建立的关键所在。

（四）建立咨询制度，构筑全方位立体化监管体系

欧盟DPIA制度一改传统数据保护的静态监管模式，由于存在数量可观的数据处理行为，且信息传播风险具有广泛性和未知性，相比于事后惩戒机制，数据保护影响评估机制注重损害发生前的评估和管理，是数据保护的最佳方案。

相比于欧盟的 DPIA 制度，我国《评估指南》在评估流程设计上缺乏根据实际风险程度决定是否向监管机构进行咨询的事前咨询制度。《个人信息保护法》第64条仅对执法部门在发现个人信息处理活动存在较大风险以及信息安全事件后的补救措施进行规定，却未对数据控制者或处理者在未发生数据安全事件前的事前咨询、上报风险等作出相关规定。数据控制者或处理者向监管机构进行事前咨询、上报风险并寻求建议等过程，必然能够大大提升数据安全风险评估的实施过程的实效性[15]。尽管《个人信息保护法》第60条规定，由国家网信部门负责统筹，国务院相关部门以及县级以上地方人民政府有关部门进行监督管理，但面对如此权责不清、管辖竞合，监管主体缺位的问题依然存在。

从实践来看，由于审计线索不足而导致的数据泄露是危害数据安全的重要因素之一，监控整个组织中的数据操作是追查取证的重要手段。一旦无法监视数据和操作合规性异常、无法收集数据活动审计的详细信息，就会造成数据泄露无法追溯，产生严重的组织风险。数据安全审计是指审计机关遵循大数据理念，运用数据技术方法和工具，利用数量巨大、来源分散、格式多样的经济社会运行数据，开展跨层级、跨地域、跨系统、跨部门和跨业务的深入挖掘与分析，提升审计监督能力和效率。《网络数据安全管理条例（征求意见稿）》第58条中提出，国家建立数据安全审计制度。可见，我国可以考虑建立通过委托第三方机构对包括但不限于企业的数据安全情况、自身承诺执行情况以及数据安全风险评估情况进行合规审计的数据安全审计制度。审计标准可以参考，如中国注册会计师协会、国际标准化组织认证制度或具有公认的隐私数据认证，以及符合国际标准化组织IEC17020质量管理体系标准[16]。

因此，建议国家建立统一的数据安全风险评估处理平台，企业将具有法律效力的数据安全审计报告上传至统一平台，将负责个人信息保护的部门业务进一步细化，构筑一个广泛使用、横纵交织的数据安全风险评估监管体系，如此方能兼顾可操作性和经济性、效率和公平。

六、结语

区别于传统的风险评估，欧盟DPIA制度通过直接设定个人数据处理环节的具体行为规范，即直接明确“规定动作”，要求数据控制者或处理者通过事前评估“规定动作”得出“自选动作”。其超越“静态底线式”的风险保护路径，对日益复杂化、泛在化、链条化的数据处理活动的数据风险防控起到了至关重要的作用，从而取得动态优化式的权益保护效果。在我国以数字经济转型推动经济高质量发展的宏观背景下，借鉴欧盟DPIA制度是我国完善数据安全风险评估标准、构建数据安全风险评估制度的可行途径。这也是强化安全等级保护、完善数字经济治理的必然要求。我国在实施《数据安全法》时，应结合实践情况不断完善评估流程设计、构建全方位监管体系，以提升数据安全风险评估质效、全面维护国家数据安全。

注释

① Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

② PbD 即“Privacy by Design”的缩写，其字面意思是“隐私保护设计”。PbD是目前国际隐私保护实践中所共同推崇的理念，它是个人信息保护链条上的第一环，要求以技术手段运用到产品和服务的形态设计中。GDPR第25条明确要求，数据控制者应须遵守“设计及默认的数据保护”（data protection by design and by default,“DPbDD”）义务，并采取适当的措施和必要的保障。

参考文献

[1] CLARKE R. Privacy impact assessment: its origins and development[J]. Computer Law & Security Review, 2009, 25(2): 123-135.

[2] WRIGHT D. The state of the art in privacy impact assessment[J]. Computer Law & Security Review, 2012, 28(1): 54-61.

[3] 谢宗晓, 董坤祥, 甄杰. 隐私影响评估(PIA)的发展及ISO/IEC 29134: 2017实施探讨[J]. 中国质量与标准导报, 2020(3): 17-20.

(下转第52页)