

个人信息保护影响评估的适用

适用场景的识别与未评估的后果

赵跃

(安徽国运律师事务所, 安徽 合肥 230000)

摘要: 个人信息保护影响评估, 是个人信息保护法确立的事前风险控制工具。该法第五十五条列举了五类应当事前评估的情形, 第五十六条规定了评估的三项内容与报告保存三年的义务。条文简约, 适用中的问题却不少: 五类情形的关系是并列还是例示; 自动化决策的评估与算法备案如何区分; 委托处理中的评估义务由谁承担; 未评估的处理活动是否当然违法; 评估报告在民事案件中具有何种证据效力。本文认为, 影响评估的性质, 是处理者的自我规制义务, 而非行政许可是前提。其规范目的在于把风险控制的关口前移, 使处理者在处理之前识别风险、设计措施。在适用场景上, 五类情形应作目的性扩张解释, 以对个人权益有重大影响为实质标准, 避免列举的封闭化。在评估内容上, 三项内容构成风险识别、风险评价与风险控制的三段结构, 其中措施与风险的相适应是核心。在后果上, 未评估不导致处理行为无效, 但构成违法处理, 处理者须承担行政责任与过错推定下的民事责任; 在公益诉讼中, 未评估可以作为过错与危险的重要证据。

关键词: 个人信息保护; 影响评估; 敏感个人信息; 自动化决策; 过错推定

中图分类号: D923 **文献标识码:** A **文稿编号:** WJLT(2025)04-0001-12

Application of Personal Information Protection Impact Assessment

ZHAO Yue

(Anhui Guoyun Law Firm, Hefei 230000, Anhui, China)

Abstract: Personal information protection impact assessment is an ex ante risk control instrument established by the Personal Information Protection Law. Article 55 lists five situations requiring assessment, and Article 56 prescribes three assessment contents plus a three-year retention duty. The provisions are brief, yet application raises many questions: whether the five situations are cumulative or exemplary; how assessment of automated decision-making differs from algorithm filing; who bears the duty in entrusted processing; whether processing without assessment is automatically unlawful; and what evidentiary weight an assessment report carries in civil litigation. This article argues that impact assessment is a self-regulatory duty of the processor rather than a precondition of administrative permission, aimed at moving risk control upstream so that risks are identified and measures designed before processing begins. The five situations should be interpreted purposively, with significant impact on individual rights as the substantive criterion, lest the list become closed. The three contents form a sequence of identification, evaluation and control, with proportionality between measures and risks at the core. Failure to assess does not invalidate processing, but constitutes unlawful processing entailing administrative liability and civil liability under a presumption of fault; in public interest litigation it serves as important evidence of fault and danger.

Key words: personal information protection; impact assessment; sensitive personal information; automated decision-making; presumption of fault

说明: (本文为作者个人研究观点, 不代表所在单位意见)

作者简介: 赵跃, 安徽国运律师事务所执业律师, 主要研究个人信息保护与数据权益纠纷的裁判规则。

一、问题的提出

个人信息保护法于2021年施行, 确立了处理个人信息的规则体系。体系之中, 影响评估是一项特殊的制度: 它不规制处理行为本身, 而规制处理之前的决策过程。

该法第五十五条规定, 处理个人信息有下列情形之一的, 应当事前进行个人信息保护影响评估, 并对处理情况进行记录: 处理敏感个人信息; 利用个人信息进行自动化决策; 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; 向境外提供个

人信息；其他对个人权益有重大影响的个人信息处理活动。

第五十六条规定，个人信息保护影响评估应当包括下列内容：个人信息处理目的、处理方式等是否合法、正当、必要；对个人权益的影响及安全风险；所采取的保护措施是否合法、有效并与风险程度相适应。评估报告和处理情况记录应当至少保存三年。

两条规范，构成了影响评估的制度框架。框架的骨架清晰，血肉却单薄。五类情形如何识别，三项内容如何展开，评估的时点与更新如何把握，未评估的后果如何，条文均未详述。

实务中的问题，集中在五个方面。第一，五类情形是并列列举还是例示概括，第五项的兜底条款如何适用。第二，自动化决策的评估，与互联网信息服务算法推荐管理规定中的算法备案，是何关系。

第三，委托处理中的评估义务，由委托方承担还是由受托方承担，双方均须评估还是仅一方评估。第四，未评估的处理活动，是无效、可撤销，还是仅承担行政责任。第五，评估报告在民事诉讼中，具有何种证据效力，能否作为过错的证明。

五个问题，指向同一个核心：影响评估的性质是什么。若它是行政许可的前提，未评估则处理行为违法无效；若它是自我规制的义务，未评估则仅生责任，不影响行为的效力。

学理上，对性质有三种主张。第一种认为，影响评估是行政监管的延伸，具有公法义务的性质。第二种认为，影响评估是处理者的内部治理，具有自我规制的性质。第三种认为，影响评估是二者兼具，既是公法义务，也是私法上的注意义务。

本文赞同第三种主张，并进一步认为，影响评估的核心是私法上的注意义务。公法义务的违反，产生行政责任；注意义务的违反，产生过错推定下的民事责任。二者的结合，构成了完整的责任体系。

本文的结构如下：第二节讨论影响评估的制度定位，第三节讨论适用场景的识别，第四节讨论评估内容的构造，第五节讨论评估的时点与更新，第六节讨论未评估的法律后果，第七节讨论评估报告的证据意义，第八节讨论与相关制度的衔接，第九节为结语。

讨论之前，须先厘清概念的层次。影响评估与安全评估、合规审计、算法备案，是四个不同的制度。名称相近，功能各异，混同适用会导致义务的错配。

影响评估的对象，是处理活动对个人权益的影响；安全评估的对象，是数据出境的安全风险；合规审计的对象，是处理者合规体系的有效性；算法备案的对象，是算法机制的安全性与可控性。四者的对象不同，方法也不同。

二、影响评估的制度定位

影响评估的制度渊源，可以追溯到环境影响评价。二十世纪七十年代，美国的环境政策法确立了环境影响评价制度，要求重大行为在实施前评估其对环境的影响。这一制度后

来被引入数据保护领域。

欧盟通用数据保护条例第三十五条确立了数据保护影响评估制度，要求在处理可能对自然人的权利与自由造成高风险时，在处理之前进行评估。评估的内容包括处理的系统性描述、必要性与相称性评估、风险缓解措施。

我国的影响评估制度，借鉴了域外的经验，也有自身的特色。特色之一，是把评估义务与处理场景绑定，以列举的方式明确五类情形。特色之二，是把评估与记录结合，要求保存三年。

影响评估的规范目的，可以从三个层面理解。第一个层面，是风险的前移控制。处理活动一旦开展，损害往往难以逆转。评估使处理者在处理之前识别风险，设计措施，从源头上减少损害。

第二个层面，是决策的理性化。评估要求处理者把处理的必要性、影响与措施书面化，使决策有据可查。书面的要求，促使处理者审慎思考，避免草率决策。

第三个层面，是问责的基础。评估报告是处理者履行义务的证明，也是监管机关与法院判断过错的依据。没有评估，处理者难以证明其已尽注意义务。

三个层面，共同决定了影响评估的性质。它不是行政许可，不需要事前审批；它是过程义务，要求处理者在决策时履行；它是问责工具，为事后追责提供依据。

明确性质的意义，在于确定未评估的后果。若评估是许可前提，未评估则处理行为违法，可能无效；若评估是过程义务，未评估则处理行为仍有效，但处理者须承担责任。

本文认为，后一种理解更为妥当。理由是：法律未规定未评估的处理行为无效，也未规定评估是处理的前置审批。从体系上看，影响评估属于处理者的自律机制，而非行政机关的准入控制。

影响评估与告知同意，是两个并行的制度。告知同意解决的是处理的正当性基础，影响评估解决的是处理的风险控制。二者不可替代。

取得同意，不免除评估义务；完成评估，也不免除告知义务。二者的关系是并列，不是选择。实务中，有处理者以已取得同意为由主张免除评估，这是对制度的误读。

影响评估与处理规则的关系，也须辨明。处理规则解决的是何种处理被允许，影响评估解决的是允许的处理如何控制风险。前者是边界，后者是过程。

以敏感个人信息为例，第二十九条规定须取得单独同意，这是处理规则；第五十五条规定须事前评估，这是过程义务。两项义务并行，处理者均须履行。

实务中，有处理者认为取得单独同意即可处理敏感信息，无须评估。这一理解遗漏了过程义务，属于典型的合规缺口。

影响评估的义务主体，是个人信息处理者。处理者的认定，依第七十三条，指自主决定处理目的、处理方式的组织、个人。受托处理者不是处理者。

共同处理的，各方均为处理者，均须评估。评估可以共同开展，也可以分别开展。共

同开展的，应当明确分工与责任。

影响评估的域外经验，还须注意其局限。欧盟的评估以高风险为前提，判断的标准较为抽象；我国的列举较为具体，便于操作，但弹性不足。

两种模式的优劣，取决于法治的阶段。列举的模式，适合规则初建的阶段；抽象的模式，适合规则成熟的阶段。我国目前宜采列举为主、兜底为辅。

兜底条款的解释，可以借鉴高风险的概念。高风险，指处理活动可能对个人的权利与自由造成重大影响，尤其是因系统性的、大规模的自动化处理而产生的影响。

三、适用场景的识别

五类情形的识别，是适用的第一步。识别的标准，须兼顾文义与目的。文义提供边界，目的提供方向。

第一类，是处理敏感个人信息。敏感个人信息的范围，依第二十八条，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

敏感性的判断，采客观标准与主观标准结合。客观上，信息一旦泄露或者非法使用，容易导致人格尊严受到侵害或者人身、财产安全受到危害；主观上，处理者应当预见特定场景下的敏感程度。

实务中的难点，是场景的叠加。单条信息不敏感，多条信息结合后敏感。例如，姓名与手机号单独不敏感，与行踪轨迹结合则可能构成敏感信息。处理者应当依处理的全流程判断，不能割裂观察。

第二类，是利用个人信息进行自动化决策。自动化决策，指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

自动化决策的典型，是个性化推荐与算法定价。前者影响个人接收的信息，后者影响个人的交易条件。二者均须评估。

评估与算法备案的关系，须辨明。算法备案依互联网信息服务算法推荐管理规定，向网信部门备案；影响评估依个人信息保护法，由处理者自行开展。二者的性质不同，不能相互替代。

实务中，有处理者以已完成算法备案为由，主张免除评估义务。这一主张不能成立。备案审查的是算法的机制，评估审查的是对个人权益的影响。审查的对象不同，结论不能互换。

第三类，是委托处理、向他人提供、公开个人信息。三种行为的共同点，是个人信息脱离原处理者的控制。控制的丧失，意味着风险的增加。

委托处理的评估，义务主体是委托方。理由是：委托方决定处理的目的与方式，受托方仅依指示处理。风险的源头在委托方，评估的义务也应由委托方承担。

但受托方也有配合的义务。受托方应当提供必要的信息，协助委托方评估。受托方另行处理个人信息的，须自行评估。

向他人提供的评估，义务主体是提供方。提供方应当评估接收方的处理能力、处理目的、保护措施。接收方再提供的，须另行评估。

公开个人信息的评估，要求更高。公开使信息处于不特定多数人可获取的状态，风险难以控制。评估应当特别审查公开的必要性及范围的适当性。

第四类，是向境外提供个人信息。此类评估与数据出境安全评估的关系，是最容易混淆的问题。二者的对象不同：前者评估对个人权益的影响，后者评估出境的安全风险。

二者的适用关系，是并行而非替代。向境外提供个人信息的，既须依第三十八条选择出境路径，也须依第五十五条开展影响评估。两条义务，均须履行。

第五类，是其他对个人权益有重大影响的处理活动。兜底条款的适用，须有实质标准。本文主张，以处理的规模、敏感程度、对个人生活的影响程度为判断要素。

规模的要件，可以参考处理的人数。处理百万人以上个人信息的，一般认定有重大影响。敏感程度与影响程度，须结合具体场景判断。

兜底条款的适用，应防止两种倾向。一种是把一切处理活动都纳入评估，导致义务的泛化；一种是把兜底条款虚置，导致列举的封闭。两种倾向，都不符合立法目的。

场景识别的另一个难点，是关联场景的判断。单一业务不构成五类情形，多项业务结合后可能构成。例如，购物平台的信息本身不敏感，但与支付信息、位置信息结合，即可能构成敏感信息。

处理者应当以产品或者服务为单位整体判断，不能以单个功能为单位割裂判断。整体的判断，符合信息聚合的风险特征。

集团内部的共享，是否构成向他人提供，须具体分析。关联公司之间共享个人信息，若各自为独立的处理者，构成提供，须评估；若为同一处理者的不同部门，不构成提供。

判断的标准，是处理目的的自主性。能够自主决定处理目的的，为独立的处理者；不能自主决定的，为同一处理者的组成部分。

自动化决策的评估，还须注意拒绝权的安排。第二十四条规定，个人有权拒绝仅通过自动化决策的方式作出决定。评估应当审查拒绝机制是否有效。

拒绝机制的有效性，包括渠道的畅通、响应的时限、替代方案的提供。渠道不畅通或者响应不及时，机制无效，评估不能通过。

自动化决策的信息推送，还须提供不针对个人特征的选项，或者提供便捷的拒绝方式。评估应当审查选项的设置是否显著、操作是否简便。

四、评估内容的构造

第五十六条规定的三项内容，构成了评估的三段结构：合法性审查、风险评价、措施

审查。三段依次递进，缺一不可。

第一项内容，是处理目的、处理方式是否合法、正当、必要。合法，指有法律依据或者取得同意；正当，指目的特定、明确；必要，指限于实现目的的最小范围。

必要性审查，是三项内容中最实质的部分。审查的方法，是比例原则：目的与手段须相当，损害须最小。具体的审查，包括信息的类型、数量、保存期限、处理频率。

实务中，必要性审查常流于形式。评估报告往往只写已取得同意、已告知目的，未真正审查必要范围。这一倾向，使评估失去了实质意义。

本文主张，必要性审查应当具体化。评估报告应当载明：处理的信息项与目的的对应关系；不处理某项信息对目的的影响；保存期限的确定依据；删除机制的安排。

第二项内容，是对个人权益的影响及安全风险。影响包括对人格尊严、人身安全、财产安全的影响；风险包括泄露、篡改、丢失、滥用的风险。

影响的评价，须区分影响的对象与程度。对象包括信息主体、第三人、社会公众；程度分为轻微、一般、严重。评价的方法，可以采用风险矩阵。

风险的评价，须考虑风险发生的可能性与后果的严重性。可能性的判断，参考信息的敏感程度、处理的环境、内部人员的接触范围；严重性的判断，参考信息泄露后的后果。

第三项内容，是保护措施是否合法、有效并与风险程度相适应。相适应，是三项内容的核心，也是评估的落脚点。

相适应的判断，采风险导向的思路：风险越高，措施越严。高风险的处理，须有加密、去标识化、访问控制、审计日志等多重措施；低风险的处理，一般措施即可。

措施的合法性，指措施本身不违法。例如，以过度收集信息作为风控手段，措施本身即违法，不能以风险为由正当化。

措施的有效性，指措施能够实际降低风险。评估报告应当说明措施的作用机理，不能只列举措施的名称。列举而无机理，是形式主义的评估。

三项内容之外，评估还应当包括处理情况的记录。记录的内容，包括处理的目的、方式、信息的类型、保存期限、接触人员、安全措施。记录的作用，是使处理过程可追溯。

记录保存三年，是法定的义务。三年的起算，从处理活动结束后之日起。处理活动持续的，从最后一次处理之日起。保存的方式，可以是电子，也可以是纸质。

三年的期限，与诉讼时效的衔接，值得注意。个人信息侵权的一般时效为三年，从知道或者应当知道权利受损之日起算。评估报告的保存期限与时效期间相近，便于诉讼中的取证。

个人信息保护影响评估的适用场景，实务中的梳理可参见

个人信息保护影响评估的适用场景，实务中的梳理可参见什么情况必须做个人信息保护影响评估：五类场景与操作一文的归纳，本文不再重复其场景清单，只就评估内容与法律后果展开。

必要性审查的具体方法，可以采四步法。第一步，明确处理的目的；第二步，列举实现目的所需的信息项；第三步，逐项审查是否必要；第四步，审查保存期限是否必要。

四步法的核心，是逐项审查。整体的审查容易流于空泛，逐项的审查才能发现过度收集。审查的结论，应当书面记载。

替代方案的审查，是必要性审查的延伸。若以较少的信息即可实现目的，则较多的收集不必要。替代方案的审查，促使处理者选择损害最小的方案。

风险的等级划分，可以采用三级制：高、中、低。高风险的，须采取多重措施并经负责人确认；中风险的，须采取基本措施；低风险的，一般措施即可。

等级的划分标准，由行业组织制定指南。指南的制定，应当结合行业的特点，避免一刀切。监管机关可以对指南进行指导。

五、评估的时点与更新

评估的时点，条文表述为事前。事前，指处理活动开始之前。开始之前的判断，以首次处理之时为准。

实务中的难点，是处理活动的连续性。产品迭代、功能上线、场景扩展，是否须重新评估。本文主张，以处理的实质变化为标准。

实质变化，指处理目的、处理方式、信息类型、共享对象发生重大变化。变化足以影响原有的风险评价的，须重新评估。轻微的变化，可以补充记录，不必重新评估。

重新评估的时点，应在变化实施之前。先实施后评估，违背了事前的规范意旨。已经实施的，应当立即补评，并采取措施控制风险。

定期评估的要求，法律未作规定。本文主张，高风险的处理活动应当定期评估，间隔不超过两年。理由是：技术环境与风险状况会变化，定期评估可以及时发现新的风险。

评估的主体，是处理者。处理者可以自行评估，也可以委托专业机构评估。委托评估的，责任仍由处理者承担。

委托评估的，处理者应当向受托机构提供真实、完整的信息。提供不实信息的，评估结论不可靠，处理者不能以已委托评估为由免责。

评估的内部程序，法律未作规定。本文主张，评估应当由专门的人员或者机构负责，评估结论应当经负责人确认。确认的程序，可以使评估具有组织上的保障。

评估的文档管理，也须规范。评估报告、处理记录、措施清单、复核意见，应当归档保存。归档的制度，便于监管检查与诉讼取证。

相适应原则的运用，还须注意措施的边际效用。措施增加到一定程度，效用递减。评估应当选择效用最高的措施组合，而非简单堆叠。

措施的记录，应当具体。仅写已加密、已脱敏，不足以证明措施的落实。应当载明加密的算法、密钥的管理、脱敏的字段、访问的权限。

第三项内容的审查，还应当包括措施的持续有效性。一次评估通过，不等于永久有效。技术环境变化、攻击手段升级，措施可能失效。定期复核，是保持有效性的必要环节。

评估报告的结构，可以参照通用的框架：处理的描述、必要性的论证、风险的识别、风险的评价、措施的设计、结论与建议。六个部分，构成了完整的报告。

结论的表述，应当明确。通过的，写明通过的条件；不通过的，写明改进的措施与时限。模糊的结论，无法指导实践。

六、未评估的法律后果

未评估的后果，是本文的核心问题。后果的设计，须兼顾三对关系：行政责任与民事责任、行为效力与赔偿责任、处理者与信息主体。

第一个后果，是行政责任。依第六十六条，违反本法规定处理个人信息或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

情节严重的，由省级以上部门责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

未评估属于未履行保护义务，可以适用上述规定。处罚的轻重，依情节确定。情节的认定，考虑处理的信息类型、数量、影响范围、是否造成实际损害。

第二个后果，是民事责任。依第六十九条，处理个人信息侵害个人信息权益造成损害，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。

这一条确立了过错推定。处理者须证明自己没有过错，才能免责。未评估的，难以证明已尽注意义务，通常认定有过错。

过错推定的正当性，在于举证能力的悬殊。处理者掌握处理的全过程，信息主体难以知悉内部的技术与管理。由处理者举证，符合公平原则。

未评估与过错的关系，须具体分析。未评估本身不等于有过错，但可以作为过错的重要证据。处理者能够证明即使评估也无法避免损害的，可以减轻或者免除责任。

第三个后果，是行为的效力。未评估的处理行为，是否无效。本文主张，不当然无效。理由是：法律未规定无效，且无效将影响大量已完成的交易，不符合比例原则。

但未评估可能影响行为的合法性。在行政诉讼中，行政机关可以据此认定处理行为违法；在民事诉讼中，法院可以据此认定处理者有过错。效力的评价，须结合具体的请求。

信息主体的请求权，包括停止侵害、删除、更正、赔偿损失。未评估的，信息主体可

以请求停止处理，但须证明处理的违法性或者损害的现实危险。

公益诉讼中的后果，值得注意。依第七十条，个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。

在公益诉讼中，未评估是重要的证据。它证明处理者未尽风险控制义务，可以作为认定违法与危险的依据。评估报告的缺失，往往使处理者处于不利地位。

行政处罚的裁量，也须规范化。未评估的，一般责令改正；造成损害的，可以并处罚款；情节严重的，可以责令暂停业务。裁量的基准，宜由部门规章明确。

民事赔偿的计算，是另一个难点。个人信息侵权的损害，往往难以量化。法院可以采用法定赔偿、酌定赔偿的方式，参考处理的规模、过错的程度、获利的数额。

精神损害赔偿的适用，须谨慎。个人信息侵权造成严重精神损害的，可以支持。严重的认定，参考信息的敏感程度、传播的范围、后果的严重性。

惩罚性赔偿的适用，法律未作规定。本文认为，恶意大规模处理个人信息造成严重后果的，可以探索惩罚性赔偿，但须有法律的明确授权。

七、评估报告的证据意义

评估报告在诉讼中的地位，是实务中的新问题。它既不是鉴定意见，也不是书证的一般形态，而是处理者自己制作的专业文件。

本文认为，评估报告的性质，是处理者的陈述性证据。它记载处理者的评估过程与结论，可以作为证明其已尽注意义务的依据。

评估报告的证明力，须具体判断。自行评估的报告，证明力较弱；委托专业机构评估的报告，证明力较强；经监管部门认可的评估，证明力更强。

评估报告的内容，影响证明力。内容具体、方法科学、数据完整的报告，证明力强；内容空泛、方法简单、结论武断的报告，证明力弱。

评估报告的提出，须注意两点。第一，报告应当完整，不得选择性提交。第二，报告应当附具评估的方法与依据，便于对方质证。

对方对报告有异议的，可以申请鉴定，也可以申请法院调查。法院应当审查报告的形成过程、方法的科学性、结论的合理性。

评估报告与商业秘密的关系，须平衡。报告可能包含处理者的技术方案与商业信息。提交时，可以申请不公开质证，或者要求签署保密承诺。

评估报告的缺失，产生举证的不利后果。处理者未评估的，难以证明已尽注意义务，法院可以推定其有过错。推定的效果，可以因处理者的其他证据而推翻。

其他证据，包括安全措施的技术文档、内部管理制度、员工培训记录、安全事件的处置记录。这些证据可以佐证处理者已尽注意义务，但不能替代评估。

八、与相关制度的衔接

衔接的作业，须明确各制度的边界与交集。边界不清，义务便会重叠或者遗漏。

第一组衔接，是影响评估与数据出境安全评估。二者的对象不同，程序不同，主管机关不同。出境的场景，两条义务并行。

实务中，有处理者以已完成安全评估为由，主张免除影响评估。这一主张不能成立。安全评估审查的是出境的安全，影响评估审查的是对个人权益的影响。

第二组衔接，是影响评估与合规审计。审计的对象是合规体系，评估的对象是具体的处理活动。审计可以发现评估的缺失，评估可以为审计提供素材。

审计的频次，依规定为定期；评估的频次，依处理的变化。二者的节奏不同，可以相互配合。

第三组衔接，是影响评估与告知同意。同意解决正当性，评估解决风险控制。取得同意不免除评估，完成评估不免除告知。

第四组衔接，是影响评估与算法备案。备案是行政程序，评估是自律程序。备案不免除评估，评估不替代备案。

第五组衔接，是影响评估与网络安全等级保护。等级保护的对象是网络系统，评估的对象是处理活动。系统的安全是评估的前提，评估的结论可以指导系统的加固。

衔接的关键，是建立统一的合规台账。处理者应当把评估、审计、备案、等级保护的材料统一管理，形成完整的合规档案。台账的制度，可以避免遗漏，也便于监管检查。

评估与保险的关系，值得关注。网络安全保险可以分散处理者的风险，保险的费率与评估的结论挂钩。评估良好的，费率较低；评估缺失的，费率较高。

这一机制，使评估获得了市场的激励。激励的引入，比单纯的处罚更为有效。监管与市场的结合，是个人信息保护的可行路径。

行业自律的作用，也不可忽视。行业协会可以制定评估的指南、发布最佳实践、组织培训。自律的补充，可以降低监管的成本。

评估的成本，是中小企业的负担。本文建议，对中小企业提供简化的评估模板与公共的技术支持，降低合规成本。分层的要求，符合比例原则。

跨境业务的评估，还须考虑法律冲突。不同法域的要求不同，评估的标准须兼顾。相互承认的机制，可以降低重复评估的成本。

最后须强调，评估不是终点，而是起点。评估的结论须落实到措施，措施须落实到运行，运行须落实到监督。闭环的管理，才是有效的合规。

评估的独立性，也须保障。评估人员应当独立于业务的推动者，不受商业目标的干扰。独立的安排，可以是设立专门的保护负责人，也可以是外部机构的介入。

保护负责人的职责，依第五十二条，包括监督个人信息处理活动、开展教育培训、提出整改建议。评估是其职责的重要组成部分。

保护负责人的独立性，须有制度保障。任命须经监管备案，解聘须有正当理由，履职须有资源支持。三项保障，是独立性的基础。

评估与监管的互动，也须畅通。监管机关可以要求处理者提交评估报告，就可以就评估的结论提出意见。互动的机制，可以使评估不流于形式。

监管的抽查，是一种有效的督促。抽查的比例不必高，但抽查的后果须明确。抽查不合格的，应当责令整改并公开。

公开的制度，可以形成声誉的约束。评估的结论，可以在年度报告中披露。披露的内容，包括评估的范围、主要风险、措施与改进。

声誉的约束，往往比处罚更为有效。消费者会用脚投票，投资者会调整估值。市场的压力，促使处理者认真评估。

评估的文化，也须培育。合规不是负担，而是竞争力。把评估视为提升产品信任度的工具，而非应付监管的手续，是合规文化的核心。

评估的失败案例，也值得总结。常见的问题有四：流于形式，照抄模板；范围不全，遗漏场景；风险低估，措施不足；文档缺失，无从追溯。

四个问题，指向同一个根源：把评估当作程序，而非实质的风险控制。纠正的路径，是把评估嵌入产品的研发流程，成为设计的组成部分。

嵌入的方式，可以是隐私设计。隐私设计主张，保护应当在系统设计的初期即予考虑，而非在事后补救。影响评估是隐私设计的工具。

隐私设计的落实，须有流程的支撑。需求阶段识别风险，设计阶段落实措施，上线阶段复核效果，运行阶段持续监测。四个阶段，构成闭环。

闭环的管理，比单次的评估更为有效。单次的评估只能解决一时的问题，闭环的管理才能应对持续的变化。

流程的支撑，还须有工具的支持。评估的模板、风险的库、措施的清单，可以减少重复劳动，提高评估的质量。

工具的建设，可以由行业组织牵头，也可以由监管机关提供。公共工具的供给，可以降低中小企业的合规成本。

最后须指出，评估的效力最终取决于执行。纸面的报告不能保护个人信息，落实的措施才能。执行的文化，是制度的生命。

本文的讨论，立足于现行的规范。随着细则的出台与实践的积累，评估的标准将更为明确，适用的争议将逐步减少。

需要补充的是跨境场景的评估叠加。向境外提供个人信息，既要依第三十八条完成出境路径的选择，又要依第五十五条开展影响评估，两条义务并行不悖。

实务中常见的错误，是以安全评估申报材料替代影响评估报告。两份文件的审查对象不同，前者审查出境的安全风险，后者审查对个人权益的影响，不能相互替代。

正确的做法，是在安全评估的申报材料之外，单独形成影响评估报告，并在报告中说明与安全评估结论的衔接关系。两份文件互为补充，共同构成出境合规的完整证明。

九、结语

个人信息保护影响评估，是事前风险控制的制度。它的价值，不在于形成一份报告，而在于促使处理者在处理之前审慎思考。

本文的主张，可以概括为三句话：以目的性扩张识别场景，以三段结构展开内容，以过错推定配置后果。三句话，构成了适用的框架。

在场景上，五类情形应作目的性扩张，以对个人权益有重大影响为实质标准。兜底条款的适用，须有规模、敏感程度、影响程度的支撑，防止泛化与虚置。

在内容上，三项内容构成合法性审查、风险评价、措施审查的三段结构。相适应是核心，风险越高，措施越严。评估报告须具体，不能流于形式。

在后果上，未评估不导致行为无效，但构成违法处理。行政责任依第六十六条，民事责任依第六十九条的过错推定，公益诉讼中未评估是重要的证据。

制度的完善，须有配套的支撑。评估的指南、行业的标准、报告的模板，三项是落地的条件。缺少任何一项，评估都可能沦为形式。

个人信息保护，是数字时代的基础命题。保护的强度，关系到人格尊严，也关系到产业的发展。影响评估的制度，正是在二者之间寻求平衡的尝试。

实务中的裁判者，面对具体的案件，须在形式合规与实质保护之间权衡，在企业发展与个人权益之间往返。这一作业，须以法理为基础，以技术为支撑。

展望未来，随着人工智能的普及与数据的跨境流动，影响评估的适用将更为广泛。评估的方法、标准与后果，都将面临新的问题。本文的讨论，仅是一个开端。

参考文献

- [1] 程啸：《个人信息保护法理解与适用》，中国法制出版社2022年版。
- [2] 张新宝：《个人信息保护法释义》，中国人民大学出版社2022年版。
- [3] 王利明：《个人信息保护的法律框架》，载《中国法学》2021年第4期。
- [4] 周汉华：《个人信息保护影响评估的制度构造》，载《法学研究》2022年第3期。
- [5] 丁晓东：《个人信息保护的风险规制路径》，载《中外法学》2021年第5期。
- [6] 洪延青：《数据出境安全评估的制度逻辑》，载《法学》2022年第7期。
- [7] 最高人民法院研究室：《个人信息保护纠纷案件裁判规则》，人民法院出版社2023年版。
- [8] 国家网信办：《个人信息保护合规审计管理办法释义》，法律出版社2024年版。