Dispute Settlement 争议解决, 2023, 9(6), 3141-3147
Published Online November 2023 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2023.96428

Hans汉斯

个人信息保护影响评估制度的困境与反思

张晓敏

上海政法学院刑事司法学院，上海

收稿日期：2023年10月12日；录用日期：2023年11月9日；发布日期：2023年11月17日

摘　要

个人信息保护影响评估制度是一种事前合规检验，在当前大数据时代，对于制约个人信息处理者的行为，保护信息主体的个人信息安全具有关键性作用。当前，我国的个人信息保护影响评估制度的有关法律规定不够完善、适用范围过于广泛、缺乏中立的监管等，这些问题可能会影响评估的公正性。为了更好发挥制度功能，切实维护个人信息安全，需要有针对性的进行完善，包括建立“三方评估体系”、设定科学合理的执行程序等，只有及时有效的完善该制度，才能确保影响评估的公正客观，预防个人信息安全遭到侵害。

关键词

大数据，个人信息保护影响评估制度，合规检验，公众参与

The Dilemma and Reflection of Personal Information Protection Impact Assessment System

Xiaomin Zhang

School of Criminal Justice, Shanghai University of Political Science and Law, Shanghai

Received: Oct. 12th, 2023; accepted: Nov. 9th, 2023; published: Nov. 17th, 2023

Abstract

Personal information protection impact assessment system is a prior compliance inspection. In the current era of big data, it plays a key role in restricting the behavior of personal information processors and protecting the personal information security of information subjects. At present,

文章引用: 张晓敏. 个人信息保护影响评估制度的困境与反思[J]. 争议解决, 2023, 9(6): 3141-3147.
DOI: 10.12677/ds.2023.96428

the relevant legal provisions of the personal information protection impact assessment system in China are not perfect, the scope of application is too wide, and the lack of neutral supervision may affect the fairness of the assessment. In order to better play the function of the system and effectively maintain the security of personal information, it is necessary to make targeted improvements, including the establishment of a "tripartite assessment system" and the setting of scientific and reasonable implementation procedures. Only by timely and effective improvement of the system can we ensure the fairness and objectivity of the impact assessment and prevent the infringement of personal information security.

Keywords

Big Data, Personal Information Protection Impact Assessment System, Compliance Inspection, Public Participation

1. 引言

个人信息保护在当前互联网时代面临新的困难和挑战，《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》)的出台具有里程碑式的意义，其中创新性地提出了一系列保护个人信息的新举措，其中的个人信息保护影响评估更是其中的亮点。本文拟对大数据时代下个人信息保护影响评估的内涵和功能进行界定，分析具体适用中存在的问题，以期为个人信息保护影响评估制度发挥其效用提供切实有效的完善措施，确保其功能的实现。

2. 概念界定

(一) 个人信息

随着大数据时代的到来，我国逐渐进入高质量发展阶段，互联网的应用和普及，对于个人信息的保护也逐渐迎来新的难题。《中华人民共和国民法典》(以下简称《民法典》)中对于“个人信息”明确给出了定义，即第一千零三十四条中规定：个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。能被称为个人信息，其中最显著的特质是该信息要具有可识别性，即社会公众根据该信息可以了解到该信息主体的一些标志性特点，具有很强的人格属性。根据此特点，法律赋予了信息主体保护其个人信息不被侵犯的一系列权利，包括未经信息主体同意不得擅自获取、已经取得的个人信息也不可未经同意被用在其他的途径等。

另外，个人信息也具有很强的公共属性。国家、政府、社会和集体可以通过收集统计个人信息来对人员进行统一调配、统一管理、统一安排，大多数情况下是被用在应急预案、疫情控制等领域。随着互联网技术的发展与应用，特定领域的相关主体可以在必要的情形下在法律规定的限度范围内收集最低限度的个人信息进行分析对比，发现客观规律，制定相关政策，解决存在的问题。正是由于个人信息本身的双重属性，即私权属性和公共属性并存，在当前大数据时代我们如何有效保护个人信息，并合理平衡两个属性[1]，是我们需要认真思考的一个难题。

(二) 个人信息保护影响评估制度

《个人信息保护法》第 55 条[1]、第 56 条[2]确定了个人信息保护影响评估制度，即我们所熟知的 PIA，规定了该制度适用的法定情形以及具体应当对什么内容进行影响评估。但是，单看法条规定的内容可知，《个人信息保护法》并没有对“个人信息保护影响评估制度”的内涵作出明确界定。

有观点认为，我国的保护影响评估制度与国际上存在的隐私影响评估制度相类似。隐私影响评估制度是指在项目开始之前查明可能造成隐私受侵害的风险，它通常是针对不同的项目分别进行单个评估，而非针对一个组织；隐私影响评估的对象广泛，可能涵盖个人行为、通信内容等多个方面；隐私影响评估是在项目开始前或者至少与项目同时进行，即事先开始，具有前瞻性。单从涵义上看，“个人信息”与“隐私”之间存在包含关系，我们对个人信息保护进行影响评估，其中一部分也涉及对隐私进行影响评估。

综上，结合我国的国情，本文认为个人信息保护影响评估制度是指：为了有效帮助个人信息处理者最小化或者规避风险，提前对对拟实施的个人信息处理活动可能造成的影响进行评价和估计的活动。

3. 个人信息保护影响评估必要性分析

(一) 个人信息保护的必要性

当前正处于世界百年未有之大变局，科技进步日新月异，互联网、人工智能出现在公众日常生活的方方面面，电子支付、网上购物等形式方便了我们的同时，对于我们个人信息的收集也日益全面频繁，个人信息安全面临前所未有的挑战。近年来，我国一直致力于推动数字政府建设[2]，期望通过收集整个社会的信息资源，进行分析，通过大数据治理提升全社会的整体治理水平。但是，建设数字政府意味着要大力发挥个人信息的公共属性，要充分运用科学技术汇集信息，这似乎与个人信息保护是相违背的；同时，数字政府是为了“建设人民满意的服务型政府”，其建设整体政府、合作政府的理念也给个人信息保护带来了新的挑战。

(二) 事前影响评估的必要性

个人信息保护影响评估制度是在处理个人信息的行为发生前进行评价和估计，是事前评估，具有预期性、前瞻性，该制度的功能主要体现在以下几个方面：

1) 检验对个人信息的处理是否合规

个人信息保护影响评估制度设定本身就是为了有效帮助信息处理者最小化未知的风险，即其首要功能就是合规检验[3]，即对个人信息的处理首先要合规，即使在合规的前提下也可能会有风险，这不可避免；若该处理方法本身就违规，则不被允许。个人信息保护影响评估的过程就是建立和证明合规的过程，有利于提升个人信息处理合规水平，可以减少声誉受损、高额罚款等相关成本[4]。《个人信息保护法》第 56 条规定的影响评估的内容第一条就是合规评估，这也从法律上明确了个人信息保护影响评估制度的首要功能，即对于个人信息的处理是否合法、正当、必要。

2) 识别并尽可能最小化信息处理的风险

《个人信息保护法》第四条对个人信息处理做出了界定，包括对个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。在如今的大数据时代，信息处理不可避免会带来或高或低的风险，我们进行事前影响评估就是为了在风险发生前尽可能将风险控制在最小限度内，以此来维护个人信息处理

[1]《个人信息保护法》第五十五条有下列情形之一的，个人信息处理者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：(一) 处理敏感个人信息；(二) 利用个人信息进行自动化决策；(三) 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；(四) 向境外提供个人信息；(五) 其他对个人权益有重大影响的个人信息处理活动。

[2]《个人信息保护法》第五十六条个人信息保护影响评估应当包括下列内容：(一) 个人信息的处理目的、处理方式等是否合法、正当、必要；(二) 对个人权益的影响及安全风险；(三) 所采取的保护措施是否合法、有效并与风险程度相适应。个人信息保护影响评估报告和处理情况记录应当至少保存三年。

者的合法权益。以开展评估为法律落地的抓手，让个人信息保护“关口前移”[5]，通过提前介入信息处理，来预防可能因此会带来的风险，以防在个人信息安全受到侵害时再采取救济手段，即事后救济，达不到保护个人信息的最终目的，毕竟在当今的互联网时代，个人信息一旦被泄露，其传播速度和范围都超乎想象，很难再及时有效的控制，消除其对个人信息处理者的消极影响。

3) 有效提升个人信息处理者的信息处理能力

个人信息保护影响评估制度通过对处理行为进行评估，不仅可以有效避免信息处理带来的风险，还可以进一步提升信息处理者的风险管理能力，通过事前影响评估，即使之后仍存在威胁信息安全的可能，也能有效帮助信息处理者减轻或者免除其责任。

企业开展个人信息保护影响评估的意义重大。对于国家来说，企业进行影响评估可以帮助企业评估其个人信息处理活动的合规性，同时也可以作为调查、审计、执法等的有效抗辩理由；对于企业而言，进行影响评估及时发现风险，可以有效采取应对措施，有效保障客户的个人信息安全，提升企业的声誉，增强可信度；对于客户来说，企业进行影响评估，对于保护自己的个人信息安全至关重要，可以让客户放心与企业合作，不必担心自己的合法权益会受到侵害。

个人信息保护影响评估制度是风险管理的重要手段[6]，它以“风险”为视角切入，通过对不同的个人信息的不同处理方法进行针对性评估，因地制宜，对于维护国家安全、社会安定、公民个人的合法权益具有不可替代的作用，因此，对个人信息处理进行事前的影响评估极其重要。

4. 个人信息保护影响评估制度的反思

(一) 现有规范规定情况

1) 现有规范数量少、不全面

正如前文所言，我国法律并没有对个人信息保护影响评估制度的概念作出明确界定，不同的学者有不同的意见。同时，通过检索法律文件可以发现，规定影响评估制度的法律文件较少，而且通过检索会发现其所使用的术语不统一，如在《网络安全法》第 37 条[3]称为“安全评估”，但在《互联网个人信息安全保护指南》[4]中使用的却是“个人信息安全影响评估”。这些法律法规中专业术语的混用，会给公众造成困扰；同时这些法律法规的规定过于分散，且大多数只是在其所涉及的领域内提到了风险影响评估，缺乏全面性和普遍性，不成体系。另外，这些法律法规的层级不够，部分规范属于非正式的法律规范，缺乏强制力。

2) 现有规范多为实体性规范，缺乏程序规制

《个人信息保护法》第 55、56 条的规定对个人信息影响评估制度的适用范围及适用对象进行规定，但是没有规定如何进行个人信息影响评估，其具体流程和适用方法均没有明确的规定。我国《信息安全技术个人信息安全影响评估指南》中规定了实施个人信息安全影响评估的具体流程，虽然“处理影响评估”和“安全影响评估”只有两个字的差异，但是其使用的流程和步骤是不能通用的，不同的评估所采取的方法、其侧重点以及期望得到的结果也是不一样的，所以不可直接适用，仍需要具体的法律作出程序性的规定。

(二) 评估制度适用广泛

个人信息保护影响评估的范围要合理，不能过宽或者过窄，否则过宽可能会给企业、个人信息处理

[3]《网络安全法》第 34 条：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

[4]如：在《互联网个人信息安全保护指南》中规定“在对个人信息的相关处理进行委托时，应对委托行为进行个人信息安全影响评估……”。

者等带来不必要的负担，造成社会资源浪费等负面影响，同时过宽可能会对个人信息处理者的风险管理能力要求过高，不利于其长远发展；若范围过窄，与该制度设置的初衷相违背，失去了本来的价值，不利于维护安全与稳定，会给个人信息安全带来威胁。侵犯信息主体的合法权益。

我国《个人信息保护法》第 55 条采取了列举式的方法对需要进行个人信息保护影响评估的事项逐一列举，共分为五大类，虽然都是具体的信息种类，但其兜底条款写道“其他对个人权益有重大影响的个人信息处理活动”也给了很大的发挥空间，换言之，只要认为“有重大影响”即需要进行影响评估，但是重大影响的程度是由谁来评价、何种程度属于“重大”这没有一个衡量标准，个人信息处理者或者说企业的自主决定权较大，同时也给了他们很大的违法犯罪空间。例如，只要是利用个人信息进行自动化决策即需要进行保护影响评估，这时不论该个人信息对于信息主体是否关键、无论利用的程度如何、也不管自动化决策的范围，可能加重保护影响评估责任人的义务，在客观上也很难做到。

(三) 对评估缺乏监管

1) 不强制披露

个人信息保护影响评估制度设定的目的是帮助个人信息处理者尽可能最小化或者规避因为信息处理带来的风险，仅面对信息处理者，有效维护了他们的合法权益，但对于社会公众来说，他们并不清楚该信息处理可能会给个人信息带来何种程度的风险[7]，也即无法对此个人信息处理形成监管，难以确保此次个人信息保护影响评估就是以社会公共利益为保护对象。因此，目前的个人信息保护影响评估缺乏向公众强制披露的机制，这不利于该制度的长久发展，可能会被不法者利用实施危害公共利益的行为。

2) 缺乏第三方评估机制

纵观我国对于个人信息保护影响评估的法律规定，可以发现都是属于个人信息处理者自己评估自己，即自评制度，而没有第三方的介入。但是一方主体不能“既当运动员，又当裁判员”，个人信息处理者和信息主体二者的利益方向在某种程度上本身相悖，此时让信息处理者在其中担任裁判者的角色，很难保证能作出中立的评判。另外“当局者迷、旁观者清”，个人信息处理者处于信息处理的流程之中，有时很难及时辨别新的风险，很容易依据经验等作出和之前相同的决策，不利于跳出定式思维，很难以一个第三方的中立视角综合评估影响，因此保护影响评估的结果可能也很难让人信服。

3) 缺乏外部监管

“没有监督的权力必然导致腐败”，通过检索我国目前关于个人信息保护影响评估的法律法规可以发现，并没有规定对这一行为进行外部的监管。如前所述，我国的保护影响评估是由个人信息处理者自己作出，也没有第三方主体的介入，即在“个人信息处理——个人信息保护影响评估”这个流程中只有个人信息处理者一方主体自行决定，完全没有另一方主体的制约，这很容易导致其利用权力实施不法行为。同时，由于没有外部的监管，信息主体在其合法权益受到侵害时无法及时寻求救济，只能运用传统的权利救济方式，很难有效维护其合法权益，因此，对个人信息保护处理影响评估设定外部监管非常有必要。

5. 个人信息保护影响评估制度的完善

(一) 程序方面

如前文所述，目前我国法律中对于个人信息保护影响评估的程序规定较少，在具体实施过程中会引发一系列问题和风险，因此科学合理的设定程序[8]，为个人信息处理者和社会工作提供合法合理的信息处理方式，对于维护个人信息安全至关重要的。

1) 增设法律规定

针对目前我国的法律现状，仅有《民法典》《个人信息保护法》等法律对个人信息保护影响评估做

出了规定，且存在较多问题，我们应作出有效整改。应当统一各个法律法规的术语，以减轻信息处理者识别的负担；同时应当对保护影响评估流程的多个方面进行细化，尽可能限制信息处理者的自由决定权。如可以通过设置一定的参与程序，让相关人员参与其中，包括内部相关人员和外部监管人员，集思广益，从不同的立场和角度对个人信息保护影响进行评估，制约个人信息处理者，维护信息主体的合法权益。同时，还可以设置复审程序，个人信息处理是一个动态变化的过程，随着外部环境的变化，其可能面对的风险也在不断改变，因此在必要时可以设置复审程序，让评估主体及时考虑风险变化以采取有效措施应对，保护信息安全。

2) 监督机制

a) 建立“三方评估体系”

我国目前的个人信息处理保护缺乏监管，对此我们要建立相应的监督机制。可以建立自评和他评相结合的评估制度，打破内部人员关注点闭塞的壁垒，增强对保护影响评估的关注度，要求政府、企业等对个人信息的处理进行影响评估，即设置第三方审计，从外部掌握安全风险变化。另外，第三方监管机构，仅处在监督的地位也是可以考虑的，即单独设定监督的机构，保持在客观中立的位置对个人信息保护影响评估的全程进行监督，对于信息处理者的违法行为及时进行纠正。也就是说，对于个人信息保护影响评估，我们应当建立一个“内部评估——外部审计——第三方监管”的三方评估体系，才能相互制约、相互配合，从而对信息处理保护影响得出客观准确的评估结论。

b) 允许公众参与

在环境法领域，环境影响评价制度[5] (EIA)设置了公众参与的方式以进一步促进社会全体成员参与到环境保护的工作中去，为了实现此目的，公众的知情权就应当得到充分保障，即应当通过充分公开相关信息，给予社会公众更大的空间参与到环境影响评价之中，充分保障公众的参与权与知情权。与之相类似，个人信息保护影响评估也应当如此，应当强制信息披露，充分公开评估，让公众参与其中，不仅可以实现对信息处理者的监管，还可以让公众更加了解信息处理评估的过程和方法，帮助公众做出正确决策。

(二) 实体方面

我国《个人信息保护法》第 56 条规定了进行个人信息保护影响评估的内容，如上所述，其一考察个人信息处理是否“合法、正当、必要”这是合规评估，是基本原则；其二其三考察个人信息处理的安全风险及保护措施的适配程度，属于风险评估。因此，我国的个人信息保护影响评估的内容涉及合规评估和风险评估两方面，二者都要兼顾，不可偏废。在考察个人信息处理的安全风险时，应全方位考察，不仅要考虑到对于信息主体的影响，还要关注对社会公共利益的损害程度。在考察评估采取的保护措施与风险程度是否相适应时，应当坚持必要的原则，坚持比例原则[9]，即信息处理者要在合理成本的范围内，采取切实有效的措施规避风险，保证个人信息不会遭受或者尽可能受到最小的损害。

6. 结语

在当今大数据时代，个人信息的保护面临新的困难和挑战；对于个人信息的处理也无处不在，个人信息保护影响评估制度在维护信息安全、维护公共利益方面发挥极其重要的作用，对于检验对个人信息的处理是否合规、识别并尽可能最小化信息处理的风险、有效提升个人信息处理者的信息处理能力等方面都发挥了关键性作用。当前，我国的个人信息保护影响评估在程序和实体等方面都存在一些问题，值得反思。我们需要不断完善法律规定的细节，明确该制度的具体适用范围及内容，设定科学合理的程序

[5]环境影响评价制度是指在进行建设活动之前，对建设项目的选址、设计和建成投产使用后可能对周围环境产生的不良影响进行调查、预测和评定，提出防治措施，并按照法定程序进行报批的法律制度。

来保证该制度功能的实现。

参考文献

[1] 胡大伟. 国有档案开放中个人信息处理活动的法理逻辑及规范架构[J]. 档案学研究, 2023(2): 59-66.

[2] 刘绍宇. 数字政府建设中个人信息保护的风险规制路径[J]. 财经法学, 2023(2): 51.

[3] 田晓华, 陈涛, 郭睿, 廖双晓, 吴强, 范歆竹. 个人信息保护合规标准实践[J]. 信息技术与标准化, 2022(5): 226.

[4] 刘权. 论个人信息保护影响评估——以《个人信息保护法》第 55、56 条为中心[J]. 上海交通大学学报(哲学社会科学版), 2022, 30(5): 39-50.

[5] 姚相振. 实施个人信息保护影响评估, 推动个人信息保护“关口前移” [J]. 中国信息安全, 2023(3): 73-75.

[6] 石佳友, 曾佳. 个人信息保护影响评估: 制度内涵与完善路径[J]. 西北工业大学学报(社会科学版), 2022(4): 90-102.

[7] 张璐. 个人信息保护风险规范的建构机理与实现路径[J]. 江西财经大学学报, 2022(3): 126-136.

[8] 董新义, 袁心悦. 个人信息保护影响评估的程序法规制[J]. 江汉大学学报(社会科学版), 2023, 40(1): 14-28.

[9] 张月昕. 大数据时代个人信息保护的困境与有效进路[J]. 中阿科技论坛(中英文), 2023(3): 158-162.