

风险管理模式下的数据保护影响评估制度

程莹

(中国政法大学人权研究院, 北京 100088)

摘要: 伴随大数据时代个人信息保护领域风险管理理论的广泛应用, 数据保护影响评估已经成为推动个人数据保护的重要制度。运用文献研究、实证分析的方法, 以 2016 年欧盟《一般数据保护条例》(GDPR) 对数据保护影响评估的规定为样本, 深入分析数据保护影响评估的理论背景、兴起与演变、含义、适用范围等内容, 以期搭建规范、明确的影响评估制度, 加强个人信息保护。数据保护影响评估内容不限于隐私风险评估, 还包括数据安全、数据质量、非歧视等内容; 对于容易带来高风险的数据处理行为, 应设定数据保护影响评估为强制性义务; 评估过程应听取利益相关者的意见, 反映其利益需求; 加强外部监督并适度公开评估报告。

关键词: 数据保护影响评估; 个人信息安全影响评估; 欧盟《一般数据保护条例》; 风险管理; 隐私影响评估; 个人信息保护

中图分类号: D920.1; C931.2

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018064

Data protection impact assessment system in the mode of risk management

CHENG Ying

Institute for Human Rights, China University of Political Science and Law, Beijing 100088, China

Abstract: In the era of big data, the risk management approach has been broadly applied in the field of personal information protection. Data protection impact assessment has become an important system to promote data protection. It takes the provisions of the data protection impact assessment of the European General Data Protection Regulation (GDPR) 2016 as the sample. By using the literature research and empirical analysis method, it analyzes in depth the theoretical background, rise and evolution, meaning and scope of data protection impact assessment to establish a standardized and specific impact assessment system as well as promote personal information protection. Assessment content includes not only privacy risk assessment, but also data security, data quality and non-discrimination. Data protection impact assessment should be set as a mandatory obligation for data processing activities that are likely to result in high risks. The evaluation process shall take the advices from stakeholders to reflect their benefits. The external supervision should be strengthened and the assessment report shall be published properly.

Key words: data protection impact assessment, personal information security impact assessment, GDPR, risk management, privacy impact assessment, personal information protection

收稿日期: 2018-06-10; 修回日期: 2018-07-15

通信作者: 程莹, yingzbj1988@163.com

基金项目: 山东省法学会法学研究课题基金资助项目(No.SLS(2017)C28); 中国国家留学基金委资助项目(No.201707070116)

Foundation Items: Law Society Law Research Foundation of Shandong Province (No.SLS(2017)C28), China Scholarship Council Foundation (No.201707070116)

1 引言

2017年12月,《信息安全技术 个人信息安全规范》(GB/T 35273-2017)^[1]等一系列国家标准正式发布,较为详细地规定了个人信息的收集、保存、使用等信息处理活动,它是对《网络安全法》等个人信息保护立法的进一步细化^{注1}。在个人信息保护法或相关司法解释出台之前,该标准是个人信息保护领域中的重要规范,不仅适用于规范各类组织个人信息处理活动,也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。值得注意的是,该标准“组织管理要求”部分,首次提出开展“个人信息安全影响评估”的要求,具体是指针对个人信息处理活动,检验其合法合规程度,判断其对个人信息主体合法权益造成损害的各种风险,以及评估用于保护个人信息主体的各项措施有效性的过程。

个人信息安全影响评估又称为数据保护影响评估或隐私影响评估,在国内是一个新概念,但在国外已有几十年的发展史,如美国、澳大利亚、加拿大等均有丰富的实践经验。经过考察、比较与借鉴^{注2},2016年欧盟《一般数据保护条例》(GDPR)第35条^{注3}确立了数据保护影响评估制度(DPIA, data protection impact assessment)。由此可见,该项制度已成为推动数据保护必不可少的重要制度。

本文拟以欧盟《一般数据保护条例》对数据保护影响评估的规定为中心,深入分析数据保护影响评估的理论背景、兴起与演变、主要内容,探讨数据保护影响评估制度中的关键性问题,吸收其最佳实践做法,以期对我国未来立法及实践提供借鉴。

2 个人信息保护理念转向——由知情同意转向风险管理

早期经济合作与发展组织指导原则、欧盟数据保护指令等个人信息保护法均制定于互联网尚未普及的年代。面对互联网大数据时代“去中心化”特点,传统的个人信息保护法遭受巨大挑战,如知情同意原则不仅给用户和机构带来沉重负担,而且流于形式,用户缺乏实际控制权。传统架构强调用户控制,然而在实践中由于缺乏可操作性,用户权利几近架空。正如有学者所说,隐私保障“承诺太多,兑现太少”^[2]。同时,大数据的出现使企业获取信息以及将信息恢复身份属性的成本正在急速下降。数据控制者,尤其是大型互联网企业对数据价值难以控制的贪念,数据控制者与数据主体间的力量悬殊,使我们不得不重新思考个人信息处理规制路径的转换^{注4}。

2015年,美国《消费者隐私权利法案(草案)》发布,运用了基于场景完整理论^[3]的风险管理模式。2016年,欧盟数据保护制度改革增设了数据泄露通知义务、数据保护影响评估义务、第三方认证等新内容,亦突出了场景导向、风险评估等新理念。风险导向的理念,即舍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,以个案分析的精神,在相应场景中具体评估数据处理行为的风险^[4]。相对于传统框架,风险管理首先承认隐私风险的必然存在,进而将隐私风险控制在可接受范围。新理念以隐私风险作为衡量个人信息“合理使用”的指标,根据具体场景中的风险评估采取差异化保障措施,变信息处理前的静态合规遵循为信息使用中的动态风险控制^[5]。有学者评价,国外个人信息保护制度的革新,以网络服务提供者主体责任的建构,特别是以其自觉履行隐私风险评估等相关义务为基础,辅之以政府监管,这是治理体系创新的最主要特征^[6]。

数据保护影响评估是落实与量化风险管理的重要手段,根据不同的风险程度,可提前预测到

注1 《网络安全法》第十五条规定,国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责,组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

注2 2011年1月,欧盟委员会发起“为数据保护和隐私权设立隐私影响评估框架”计划(PIAF),该计划调研了澳大利亚、加拿大等的隐私影响评估实践,力图搭建适于欧洲的模式框架。

注3 与GDPR序言及第29条工作组指南(Article 29 Data Protection Working Party “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ‘likely to result in a high risk’ for the purposes of Regulation 2016/679”),一并对数据保护影响评估制度进行了详细规制。

注4 近期360直播事件、支付宝年度账单事件、百度窃听事件非常直观的表明,由于个人信息收集使用的隐蔽性、即时性,单个用户的直接损害通常难以举证,因此愈难主张个人权利。

数据处理对个体权利的影响并给出风险规避建议。^[7]一方面,数据保护影响评估义务是对数据控制者责任的强化,将隐私渗透进项目而不仅仅是与项目相联系,有助于增强数据控制者的隐私风险管理责任意识,一定程度上平衡数据控制者利益与数据主体的隐私利益;另一方面,有助于维护数据控制者信誉,培育数据主体的信心。同时,个人数据的泄露和不正当使用将影响个人的习惯、偏好和自主权,甚至影响言论自由等基本人权。因此,较好地落实数据保护影响评估,满足数据主体的隐私期待,对促进金融科技、维护个人权利、推进民主有重要意义。

2.1 数据保护影响评估制度中的核心问题

数据保护影响评估的概念由隐私影响评估发展而来,而隐私影响评估起源于环境影响评估和社会影响评估^[8],兴起并成熟于1995年至2005年间。在OECD《隐私保护和个人数据跨境流通指南》之前的欧洲数据保护法一般要求对数据处理进行登记或认证,并需要对数据控制者的处理行为进行合规性审查(compliance check),这被认为是隐私影响评估的早期表现形式。随着实践的发展,法律解释及自由裁量给隐私机构提供了更多丰富隐私影响评估内涵的空间,影响评估的内涵变得比合规性审查宽泛的多。有学者早在1989年著作中提及,在一些北欧国家和英国,偶尔使用“决定前评估”(pre-decisional assessments)的概念^[9]。而首次使用“隐私影响评估”这一语词的是兰斯·霍夫曼(Lance Hoffman),其在协助起草一项要求设立隐私影响评估的加利福尼亚伯克利法令中提及此概念^[10]。之后,加拿大、新西兰和澳大利亚的一些隐私保护专家认为系统化的隐私影响评估是数据保护必不可少的工具。这一观念在政策领域迅速传播,经历五到十年的发展,隐私影响评估逐渐被规范适用^[11]。

在欧洲,隐私影响评估实践起步较晚^{注5}。1995欧盟数据保护指令^{注6}第20条规定了对信息系统,

尤其是对敏感信息系统的预先审查义务。之后,欧洲委员会开始表现出对隐私影响评估的兴趣,认为其是促进数据保护的重要机制。2011年2月,在欧洲委员会积极推动下,第29条工作组签署了《无线射频识别应用隐私和数据保护影响评估框架》。第29条工作组认为,隐私影响评估是促进依照设计的隐私(privacy by design)、为个人提供更优的信息,以及与监管机构交换意见的工具。2016年,GDPR第35条引入了数据保护影响评估制度,同时GDPR在“处理过程的安全性”“控制者的义务”等多处提及数据保护影响评估。

尽管欧洲起步较晚,但鉴于其将数据保护影响评估制度纳入立法,且充分吸收了其他国家的最佳实践做法,因此,以下主要以GDPR的规定为核心内容,探讨数据影响评估制度中的关键性问题。

2.1.1 数据保护影响评估的含义

在GDPR采用数据保护影响评估的概念之前,国外理论与实务界通常使用隐私影响评估的概念。尽管《欧盟基本人权宪章》第7条和第8条将数据保护和隐私权分两项条款加以保护,欧洲司法判例及法学研究中仍经常一并适用数据保护和隐私权的概念^[12]。而上文也提到,在GDPR数据保护影响评估制度制定的过程中,也充分吸收和借鉴了各国有关隐私影响评估的立法和实践经验。因此,在各类代表性定义中,经常将二者杂糅在一起,故在此一并对两项定义进行分析。

根据第29条工作组指南的内容,数据保护影响评估(又称为隐私影响评估或风险评估)是一种用于描述数据处理过程、评估其必要性和合比例性、协助管理对自然人权利和自由带来的风险并决定处理措施的方法^{注7}。罗尔夫教授认为,数据保护影响评估(在一定程度上又称为隐私影响评估)是一种评估有关个人数据处理组织活动的隐私风险的方法或过程^[13]。莱特等^[14]认为,隐私影响评估是一种用于评估有关个人信息处理的计划、政策、项目、服务、产品的方法,并对利益

注5 英国是欧洲第一个推行隐私影响评估的国家。英国信息委员会办公室在2007年12月发布了PIA手册(2014年修订为《隐私泄露影响评估的实践法则》)。2011年,29条工作组发布RFID(无线射频识别)应用隐私和数据保护影响评估框架。2015年,法国CNIL发布全面PIA手册,包括了方法、手段和典型的实践案例。

注6 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

注7 [Article 29 Data Protection Working Party “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ‘likely to result in a high risk’ for the purposes of Regulation 2016/679” http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

相关者进行咨询,采取必要补救措施以减少或避免负面影响。罗杰·克拉克教授一文附录1列举了6个国家或地区文件中对隐私影响评估的界定^[15]。认为它不仅仅是一项工具,更是一个过程,应当始于数据处理的最早期阶段,并能延续到数据处理结束甚至结束以后。

总体来看,数据保护影响评估应当包含以下要素。

1) 数据保护影响评估的内容不仅限于对隐私的影响评估,还包括评估数据安全、数据质量、非歧视等内容。数据安全是确保数据有效应对某些危机,如丢失或被未经授权的人获取,导致数据的非法使用。数据质量是指确保数据的准确、充分、相关且及时更新,不准确的信息会导致个人数字形象的扭曲。同时,大数据时代算法的专业性和不透明性容易导致歧视与不公,甚至受利益集团的操控,因此,对非歧视内容的关注也成为评估的重要内容。

2) 合比例性。比例原则贯穿于数据保护框架之中,并支持大多数数据处理原则的适用。如个人数据处理应当和收集、处理的目的相关并且处于最小必要范围,存储时间不能超过实现数据处理目的所必需的时间。

3) 全生命周期。数据保护影响评估应当在处理前实施,从规划、建设、运行、结束,是一项持续性的评估过程,尤其当数据处理是持续动态的并且在不断变化的时候。英国信息委员会办公室隐私影响评估实施手册中强调,数据保护影响评估是一个过程,而不单单是为了出具一份报告。即便在发布报告之后,数据保护影响评估仍应当进行。

4) 采取风险控制措施。针对评估中的高风险事项,反馈至项目最初设计环节,提出具有针对性的修改或处理方案。同时,应充分调动其他机构或人员,包括事先咨询数据保护专员、数据保护监管机构建议,制订处理方案等。

综上所述,本文认为,数据保护影响评估是指评估某一项目、服务或产品对个人隐私、非歧视、数据安全、数据质量等内容带来的风险,检验其合比例性,以制订降低风险措施的覆盖全生命周期的方法。

2.1.2 数据保护影响评估的适用范围

是否所有个人数据处理行为均需要进行数据保护影响评估,哪些必须进行数据保护影响评估,是数据保护影响评估制度的关键问题。一项完整的隐私影响评估需要耗费较高的成本,对企业产生一定的负担。以实践情况来看,英国和法国的数据保护机构均发展了各自的隐私影响评估方法。然而,大部分情况下这些方法仅作为一种建议而非法律义务。澳大利亚隐私影响评估指南指出,任何组织,一旦计划实施有可能侵害隐私的项目,均应当实施隐私影响评估,但也并未将实施隐私影响评估作为一项立法要求。

相比而言,GDPR将数据保护影响评估列为一项法定义务,但规定数据保护影响评估义务只有在数据处理的性质、范围和目的可能给数据主体的基本权利与自由造成高风险时,才要求数据控制者履行该义务。条例尤其强调新科技的应用,如应用新科技以适用于大范围数据处理,而对数据主体权利带来高风险,尤其是这些处理活动中数据主体难以主张权利时,应当适用数据保护影响评估。

GDPR第35条第3款列明了三项尤其需要数据保护影响评估的情形。

1) 基于数据的自动化处理(包括识别分析),或者基于对该自然人产生法律效力或类似的显著影响的决定,对自然人个人方面的系统和广泛的评估。尤其是有关数据主体的工作表现、经济状况、健康、个人偏好或兴趣、可信度或习惯、位置或行迹。其他可能导致对个人歧视的数据处理。比如金融机构审查客户的征信数据,生物科技公司直接对客户进行基因测试以评估其健康风险,或公司基于网站的使用记录建立个人行为档案。

2) 处理大规模的特殊类型的数据,或有关犯罪记录和违法行为的个人数据。例如,医院的病人医疗记录,私家侦探的犯罪嫌疑人信息。GDPR序言第91条认为,大范围处理活动是在区域、国家或超国家层面处理个人数据,会对大量数据主体产生影响并有可能带来重大危机的数据处理行为。在判定是否是大范围处理活动时,尤其应当考虑以下因素:相关数据主体的数量(具体数量或相关人口比率),数据总量和/或被处理的不同

数据的范围，数据处理活动的时限，处理活动的地理范围。大范围处理活动的例子有：医院患者数据，城市公共交通系统个人交通数据，基于统计目的而收集的国际快餐链中消费者实时地理位置数据，保险公司或银行顾客数据，搜索引擎为行为广告（behavioral advertisement）而进行的数据处理，电话或互联网服务提供商对数据的处理。个体医师的患者信息处理不认为是大范围个人数据处理。

3) 对公共区域大规模的系统化监控。用于对数据主体观察、监控或控制的数据处理，包括通过互联网收集数据或第35条第3款c项的对公共区域系统化的监控。这种情况下数据主体有可能无法获知谁在收集以及如何使用他们的数据。此外，个人也难以避免在公共区域发生的数据处理活动。

除此之外，还应考虑其他“有可能导致高风险”的情形。GDPR第35条第4款要求，监管机构应当确定并公开一份清单，列举应当进行数据保护影响评估的处理行为。因此，成员国可自行确定其他必须进行数据保护影响评估的情形。第29条工作组指导条例列举了几项参考标准。

1) 带有高度个人特征的数据。例如，个人文档、电子邮件、日记、随手记，以及日程记录软件中的非常私人的信息也在衡量范围。但也应当考虑这些数据是否已被数据主体或第三方公开，或这些数据是否已被允许基于特定目的的处理。

2) 相匹配或合并的数据集。例如，源于两项或多项基于不同目的的数据处理活动，由不同数据控制者运用超出数据主体合理预期的方式展开。

3) 与弱势数据主体相关的数据。75条序言认为，由于数据主体和数据控制者力量不均衡而导致个人无法轻易同意或反对数据处理。例如，儿童、雇员以及更加需要特殊保护的群体（精神病患者、寻求庇护者或老人等）。

4) 创新使用或运用新技术或组织手段。比如将指纹和脸部识别用于控制物理访问。这是因为类似技术的使用会带来数据收集和使用方式的革新，由此带来的影响是难以预期的。

5) 当数据处理阻碍数据主体主张权利或接

受服务合同时。这包括某项处理活动意在允许、变更或拒绝数据主体获得服务或签订合同，如银行审查客户征信情况以决定是否提供贷款。

在大多数情况下，数据处理如满足两项以上标准的，应要求进行数据保护影响评估。满足的条件越多，风险越大，越需要进行评估。如认为符合以上情形但不存在较大风险时，应列明不实施数据保护影响评估的原因，以及数据保护专员的意见。实践中有更为简单明了的判断方法，如澳大利亚维多利亚州隐私委员会隐私影响评估指南中建议，为决定是否有必要隐私影响评估，需要回答17项简单的问题，如所有问题均为是，则该组织应认真考虑进行隐私影响评估^[16]。

对于不需要进行数据影响评估的情形，第29条工作组列举了以下情形。

1) 数据处理的行为、范围、内容、目的和之前已经实施过数据保护影响评估的数据处理情况相似，可直接适用之前的数据保护影响评估结果。

2) 在2018年5月GDPR正式实施之前，在具体条件（如范围、目的、个人数据、数据控制者或接收者身份、数据存储期限等）未发生改变的情况下，数据处理已经通过监管机构的审查。

3) 基于数据控制者的法定义务、公共利益或履行数据控制者的职务所必要的数据处理，欧盟或成员国法律对该项处理行为做出了明确规定，要求数据保护影响评估已经实施，以作为该项数据处理的合法基础。

4) 根据第35条第5款，各成员国监管机构清单中列明的不必要进行数据保护影响评估的情形。

2.1.3 数据保护影响评估的参与主体

数据控制者负责对数据保护影响评估的实施，具体工作可以由组织内或组织外的其他个人或机构完成，但数据控制者最终对数据保护影响评估的实施情况承担责任。数据保护专员是实施数据保护影响评估的重要角色。在适当情形下，数据控制者应咨询数据保护专员的意见，相关建议及数据控制者的决定应当被录入数据保护影响评估。数据保护专员也应当监督数据保护影响评估的实施，如数据处理完全或部分由数据处理者实施，处理者应提供必要信息，协助控制者实施数据保护影响评估。

有学者认为,咨询不同的利益相关者是识别隐私问题和寻求可能解决方案的关键步骤,如缺乏明确的公众参与机制,将限制外部专家协助识别通常复杂的技术系统对隐私的影响^[17]。大卫·赖特教授等^[18]也认为,仅实施合规性审查并不足以识别对隐私的影响,应充分寻求数据主体及其他利益相关者的意见。GDPR 第 35 条第 9 款规定,在适当情况下,数据控制者应就拟进行的处理行为征询数据主体的意见。这使数据主体可以自我评估该处理行为的安全措施是否充分,并帮助其选择拥有更优隐私保障的公司。英国信息委员会办公室隐私影响评估手册中提到,利益相关人的咨询意见是一项关键性因素。除此之外,如条件允许,可考虑具有独立地位的专家(如律师、IT 专家、安全专家等)及首席信息安全专员等角色的意见。

(1) 数据保护影响评估的内容

有学者认为,隐私影响评估应当识别隐私风险以及如何降低风险的相关信息。隐私影响评估包括对范围、法律基础、系统效力以及系统对隐私利益影响的分析。隐私影响评估也应当有可能避免、减少、阻止隐私风险或建议替代性方案^[19]。

GDPR 第 35 条第 7 款规定,评估内容至少应当包括如下内容。

1) 对设想中的数据处理行为及处理目的的系统性阐述,适当的情况下还包括数据控制者追求的合法利益。

2) 基于处理目的,对处理行为的必要性及比例性的评估。

3) 对第 1 款中规定的对数据主体权利和自由产生的风险的评估。

4) 处理这些风险的预想方案,包括安全和保障措施,以及确保个人数据的保护和证明符合本条例规定的机制。

数据控制者或处理者对第 40 条规定的行为准则的遵守情况也是数据保护影响评估中应当考虑的因素。此外,是否满足认证条件、是否获得数据保护印章和标志,以及是否遵守公司约束规则,也可以作为数据保护影响评估的考虑因素。

为更规范地实施数据保护影响评估,数据保护机构在逻辑上应当提供一个综合的、可操作的

评估模型。尽管无法为所有情形提供统一标准,但大多数隐私评估指南均提供了实施方法和报告模板。在加拿大阿尔伯塔省,这种模板还是强制适用的。数据保护监管机构应当为此提供指引,以便于数据控制者可参考其他机构的经验,更有效实施数据保护影响评估。新西兰手册中便提供了国家及国际隐私影响评估的资源目录。

(2) 数据保护影响评估报告的监督

报告的公开是对数据保护影响评估进行监督的重要途径,有助于提升透明度和公众信心。政府部门可以设立数据保护影响评估注册中心,以发布典型的数据保护影响评估报告。“评估结果应当以概述形式通过中心网站公布,以便于数据主体及时查阅数据控制者的评估是否满足其利益期待^[20]。”如果报告中含有商业秘密或其他竞争性因素而不便全部公开,可在适当处理后公开,或至少公布摘要^[21]。

GDPR 没有要求数据保护影响评估报告的公开,但规定了事先咨询制度。即对于数据控制者缺乏减轻风险的措施会导致高风险时,数据控制者应当在处理前向监管机构咨询。在这种情况下,应当将数据保护影响评估报告的内容提交监管机构。监管机构应当在收到咨询请求后八周内,向数据控制者提供书面建议,如情况复杂可延长六周。该期限可暂停直到监管机构获得了基于咨询目的所要求的信息。数据控制者应向监管机构提供以下信息:①处理过程中涉及的数据控制者、共同控制者和处理者各自的责任,尤其是当处理发生在企业集团内部时;②打算实施的处理行为的目的和方法;③保护数据主体的保障措施;④数据保护专员的联系方式;⑤数据保护影响评估的内容;⑥监管机构要求的其他信息。

为确保影响评估的实施效果,有专家梳理了欧盟隐私影响评估框架中设立的评估标准,并提出了“‘隐私影响评估’评估和打分系统(PEGS)”模型,以对隐私影响评估的效果进行评估和打分,并对利益相关者可见。这种平台的设立有助于公众对隐私影响评估结果的获取,促进公众信心的建立,同时有助于不同机构间交流经验进而提升隐私影响评估水平^[22]。

对于不遵守数据保护影响评估义务的情形,

GDPR 设立了较为严苛的罚则。不执行 GDPR 第 35 条第 1、3、4 款, 或不正确执行数据保护影响评估义务(违反 35 条第 2、7、9 款), 或没有按规定咨询监管机构(违反 36 条第 3 款 e 项), 将被处以一千万欧元或全球营业额的 2% 罚款, 两者竞合取较高者。由此, 将管理成本转移到威胁源, 形成了真正的风险管理闭环。

3 对我国的借鉴价值

目前, 我国个人信息保护领域正在加紧立法。与《个人信息安全规范》相配套的国家标准《个人信息安全影响评估指南》正在制定过程中。国外数据保护影响评估制度的成功经验对于我国有重要的借鉴意义。

(1) 立法层面

个人信息安全影响评估不应仅限于国家政策层面, 应搭建从《网络安全法》个人信息保护法、个人信息安全规范、个人信息安全影响评估指南等, 从法律到政策的立体式规范架构。从法律层面确立个人信息安全影响评估的义务, 明确适用范围、评估内容及相应的处罚或赔偿条款, 在国家政策标准层面细化评估的内容、方法、程序, 提供评估模板和样本。

(2) 评估内容

标准规定, 个人信息安全影响评估是指针对个人信息处理活动, 检验其合法合规程度, 判断其对个人信息主体合法权益造成损害的各种风险, 以及评估用于保护个人信息主体的各项措施有效性的过程。从评估内容来看, 个人信息安全影响评估不仅保护个人信息安全利益, 同时保护名誉、非歧视等多种利益。总体来看, 我国规定较为全面、成熟, 但未列明对隐私利益的保护, 未突出全生命周期、利益相关者咨询等要素。

(3) 适用范围

《个人信息安全规范》中其他条款均使用了“应”一词, 而在个人信息影响评估一项中未使用, 这表明我国对个人信息安全影响评估的适用范围仍有待明确。本文认为应借鉴 GDPR 的经验, 当信息处理可能会对个人信息主体权益带来高风险时, 个人信息控制者负有风险影响评估的法定义务, 除此, 可减少或免除风险评估义务。

(4) 参与主体

对于网络安全风险评估, 我国《网络安全法》规定, 由个人信息控制者、第三方及行业组织完成。对于个人信息安全影响评估, 可充分借鉴以上经验, 一并发挥个人信息控制者、第三方、行业组织的积极作用, 但最终由个人信息控制者对评估结果承担责任。在个人信息控制者内部, 应充分发挥个人信息保护负责人和个人信息保护工作机构的作用。同时, 在适当情况下应征询个人信息主体或代表人的意见, 以更好地了解其相关利益期待。

(5) 监督

标准规定了形成个人信息安全影响评估报告的义务, 并要求妥善留存, 供相关方查阅, 并以适宜的形式公开。该规定贴近国际通行做法, 有利于提升评估效果。与此同时, 监管机构或在制订中的《个人信息安全影响评估指南》可以考虑拟定个人信息安全影响评估范本, 并可在相关网站发布典型的个人信息安全影响评估报告, 协助个人信息控制者更好完成个人信息安全影响评估。

参考文献:

- [1] 《信息安全技术 个人信息安全规范》(GB/T 35273-2017) [S]. 2018. <http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=4FFAA51D63BA21B9EE40C51DD3CC40BE>. Information security technology-personal information (GB/T 35273-2017)[S]. 2018. <http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=4FFAA51D63BA21B9EE40C51DD3CC40BE>.
- [2] RUBINSTEIN I S. Big data: the end of privacy or a new beginning[J]. International Data Privacy Law, 2013, 3(2): 74-87.
- [3] NISSENBAUM H. Privacy as contextual integrity[J]. Wash L Rev, 2004, 79: 101-139.
- [4] KUNER C, et al. Risk management in data protection (2015) 5 International Data Privacy Law 95, 98.
- [5] 范为. 大数据时代个人信息保护的路径重构[J]. 环球法律评论, 2016(5):92-115. FAN W. The path reconstruction of personal information protection in the age of big data[J]. Global Law Review, 2016(5):92-115.
- [6] 杨秀. 网络服务商个人信息保护制度的缺陷及其完善—以新浪微博诉脉脉案为例[J]. 国际新闻界, 2017(8):140-155. YANG X. Defects and perfection of personal information protection system of network service providers: take the 'sina micro-blog prosecuted maimai' as an example[J]. Chinese Journal of Journalism & Communication, 2017(8):140-155.
- [7] 张敏, 马民虎. 欧盟数据保护立法改革之发展趋势分析[J]. 网络与信息安全学报, 2016(2):00030-1. MA M, MA M H. Analysis on the development trend of EU data

- protection legislation reform[J]. Chinese Journal of Network and Information Security, 2016, 2(2): 8-15.
- [8] WADHWA K, RODRIGUES R. Evaluating privacy impact assessments[J]. Innovation: The European Journal of Social Science Research, 2013, 26(1-2): 161-180.
- [9] BENNETT C J. Regulating privacy: data protection and public policy in Europe and the United States[M]. Cornell University Press, 1992: 112.
- [10] HOFFMAN L J. Security and privacy in computer systems[M]. Los Angeles: Melville, 1973:125.
- [11] CLARKE R. Privacy impact assessment: its origins and development[J]. Computer Law & Security Review 2009,25:123-135.
- [12] DE HERT P. A human rights perspective on privacy and data protection impact assessments[C]//Privacy Impact Assessment. Springer, Dordrecht, 2012: 33-76.
- [13] WEBER R H. Privacy management practices in the proposed EU regulation[J]. International Data Privacy Law, 2014, 4(4): 290.
- [14] WRIGHT D, DE HERT P. Privacy impact assessment[M]. Springer, 2011:5-6.
- [15] CLARKE R. Privacy impact assessment: its origins and development[J]. Computer Law & Security Review 2009,25:123-135.
- [16] CLARKE R. PIAs in Australia: a work-in-progress report privacy impact assessment[M]. Springer, Dordrecht, 2012: 119-148.
- [17] BAMBERGER K A, MULLIGAN D K. Privacy decision-making in administrative agencies[J]. The University of Chicago Law Review, 2008, 75(1): 75-107.
- [18] WRIGHT D, FINN R, RODRIGUES R. A comparative analysis of privacy impact assessment in six countries[J]. Journal of Contemporary European Research, 2013, 9(1):160-180.
- [19] TANCOCK D, PEARSON S, CHARLESWORTH A. Analysis of privacy impact assessments within major jurisdictions[C]//Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on. IEEE, 2010: 118-125.
- [20] WRIGHT D, WADHWA K. Introducing a privacy impact assessment policy in the EU member states[J]. International Data Privacy Law, 2012, 3(1): 13-28.
- [21] WRIGHT D, FINN R, RODRIGUES R. A comparative analysis of privacy impact assessment in six countries[J]. Journal of Contemporary European Research, 2013, 9(1):160-180.
- [22] BAMBERGER K A, MULLIGAN D K. PIA requirements and privacy decision-making in US government agencies privacy impact assessment[M]. Springer Netherlands, 2012: 225-250.

[作者简介]



程莹(1988-)女, 山东聊城人, 中国政法大学博士生, 主要研究方向为个人信息保护和隐私权。