DOI:10.19641/j.cnki.42-1290/f.2024.08.012

个人信息保护合规审计探究

赵翰隽，殷 楠（副教授）

【摘要】个人信息保护合规审计是合规审计制度在数字及人工智能时代的延伸拓展。本文运用理论探究及规则分析等方法，深入研究个人信息保护合规审计制度的底层法理逻辑、特征属性、功能需求、指导原则等理论问题，以及合规审计的框架及方法。在提出阐释个人信息保护合规审计制度具有多重底层法理逻辑的基础上，进一步分析论证合规审计具有强烈的规则解释适用上的“裁量判断”属性，为此，建议确立和运用利益衡量上的比例原则、审计独立下的沟通及共识解释原则等指导原则。为塑造形成一个综合全面、立体多维、契合紧密、功能卓越的个人信息保护合规审计制度与机制，应逐步建立完善相关的审计框架、功能模块、指标体系、技术方法等。

【关键词】个人信息保护；合规审计；裁量判断；比例原则；数字经济

【中图分类号】F239 【文献标识码】A 【文章编号】1004-0994(2024)08-0080-6

2021年8月我国出台的《个人信息保护法》首次在法律层面提出了个人信息保护合规审计的要求，包括信息处理者定期自行安排合规审计，按照监管部门要求委托专业机构进行合规审计。2023年8月，国家互联网信息办公室进一步发布了《个人信息保护合规审计管理办法（征求意见稿）》及配套的《个人信息保护合规审计参考要点》。但是，个人信息保护合规审计制度尚处于初步建立阶段，相关工作尚处于探索实践中。为此，需要进一步分析个人信息保护合规审计制度建构运作的底层法理逻辑以及应遵循的重要原则，进一步明确、完善合规审计的规则体系和技术方法等。

一、个人信息保护合规审计制度的形成及底层法理逻辑

（一）个人信息保护合规审计制度的形成

个人信息保护合规审计制度是数字时代的产物，是在数字社会及数字经济的发展中逐步形成的。1996年，国际信息系统审计与控制协会（ISACA）发布《信息及相关技术控制目标标准》（COBIT标准，2019年）。该标准围绕着信息系统的开发运用制定了四十多项规制目标，并提出相应的审计要求与方法。目前，该标准已成为关于信息系统审计的通用标准。其中，“系统安全”与“数据管理”控制目标及审计要求涉及信息保护问题。2002年，美国国家审计署发布了《联邦信息系统控制审计手册》（2009年修订），该手册主要适用于联邦和其他政府实体的信息系统审计。2018年5月25日，欧盟《通用数据保护条例》（General Data Protection Regulation，GDPR）正式生效。在该条例的约束要求下，英、法、德等欧盟国家开始制定和实施本国的数据保护审计制度。英国的数据保护审计以自愿审计为主、强制审计为辅。其中，信息专员办公室开展的审计是一种基于监管层面的强制审计。2020年9月，法国数据保护局（CNIL）发布《CNIL审计程序指南》，阐述了数据保护合规审计的权利与义务及各种具体问题（贾丹等，2022）。这些新的审计制度有着各自特定的宗旨目标和关注重点，如信息系统审计、数据保护审计主要关注解决的是安全性、可靠性及风险防控问题，并非个人信息保护问题。但是，这些新的审计制度显然与个人信息保护问题紧密相关，个人信息保护上的诸多要求也包含在这些新的审计制度所关注的问题中，这就为个人信息保护合规审计制度的形成发展奠定了基础和关联支撑。

从全球算法治理的实践来看，其为个人信息保护合规审计制度的形成发展提供了重要的技术内核与经验支持。目前，一些大型互联网企业正在进一步研发关于算法内部审计的制度框架和技术工具。例如，Google专门研发设计了“SMACTR”的算法内部审计框架，将内部审计工作划分为五个相互衔接的阶段性框架。Meta、IBM、Google分别开发了Fairness Flow、AI 360 Toolkit、Model Card Toolkit等技术工具，用以检测、报告、减轻算法设计运用中可能存在的歧视等问题。在算法内部审计之外，监管机构也正在逐步推进开展对算法的监管审计。一种是关于算法合规问题的个案审计。例如：英国信息

【作者单位】南京审计大学法学院，南京 211815

专员办公室对Clearview AI违法处理个人数据尤其是生物特征数据的行为开展监管审计；针对Everalbum公司擅自使用用户照片及面部信息训练算法的行为，美国联邦贸易委员会开展专项审计调查。另一种是围绕算法的公平性、透明度、安全性等一般性问题进行风险评估审计（张欣和宋雨鑫，2022）。显然，个人信息保护上的许多问题往往来自于信息处理者所设计和运用的算法，算法审计的制度与实践将为个人信息保护合规审计制度的建构运作提供关键的技术内核与经验支持。

在信息系统审计、数据保护审计、算法审计等高度相关的审计制度被各国陆续建立和广泛实践的背景环境下，随着个人信息权益保护的法律观念与规则不断强化，个人信息保护合规审计制度的形成发展也就成为一种必然。2020年国家市场监督管理总局、国家标准化管理委员会制定发布的《信息安全技术 个人信息安全规范》中，第11.7条对个人信息控制者提出了开展个人信息安全审计的要求。虽然该国家标准并没有直接提出个人信息保护的合规审计要求，但在安全审计的要求下，已经涉及个人信息保护合规审计的实质要素。2021年8月通过的《个人信息保护法》首次在法律层面提出了个人信息保护合规审计的要求。该法第五十四条规定，个人信息处理者承担定期进行合规审计的法定义务；第六十四条规定，监管部门根据发现的问题，可强制要求信息处理者委托专业机构对其进行合规审计。2021年11月，国家互联网信息办公室发布了《网络数据安全管理条例（征求意见稿）》，该征求意见稿第五十三条规定，大型互联网平台应当委托外部机构对平台数据安全、个人信息保护等情况进行合规审计；第五十八条规定，国家应建立数据安全审计制度。可见，数据处理者应承担委托数据安全审计专业机构进行定期合规审计的义务，主管、监管部门应组织开展监管审计工作。显然，这是从数据安全的角度对个人信息保护提出的合规审计要求。2021年12月，国家互联网信息办公室等四个部门联合发布了《互联网信息服务算法推荐管理规定》，专门就算法推荐服务提出了合规要求。这就从算法推荐服务层面对个人信息保护进一步提出了特定的合规要求。2023年8月，国家互联网信息办公室进一步发布了《个人信息保护合规审计管理办法（征求意见稿）》及配套的《个人信息保护合规审计参考要点》。根据该征求意见稿的规定，处理超过100万个人信息的信息处理者，每年至少应实施一次合规审计；其他情形下每两年至少应实施一次合规审计。这两份文件全面细化了个人信息保护合规审计制度。总体而言，目前，以《个人信息保护法》所设定的合规审计这一法定要求为中心，以各种相关的规章和规范性文件为关联支撑并细化展开，正在逐步形成关于个人信息保护合规审计的综合全面、立体多维的规则体系。

（二）建构个人信息保护合规审计制度的多重底层法理逻辑

1. 审计制度及其功能作用适应时代延伸扩展的发展逻辑。实际上，个人信息权益保护问题并不是一个传统意义上的审计问题。根据美国会计师学会审计基本概念委员会在1972年发布的《基本审计概念说明》，审计是客观收集、评价有关经济活动和事项的证据，并确定其与已有标准的相符性的系统过程。在国内理论和立法上，审计一般是指对被审计单位的财政、财务收支及有关经济活动的真实、合法、效益进行审查监督。有研究将国家审计定义为，对受托管理和使用公共资源的责任履行情况进行的独立监督活动（刘力云等，2021）。“审计”这一特殊的概念术语表明，审计制度的核心领域与对象内容是宏观和微观的各种经济运行及其审查监督问题，其实质是监督、鉴证、评价公共受托责任的履行情况。显然，个人信息保护合规问题的核心是，分析判断个人信息权益保护的状况与效果，它应当主要属于行政执法监管和司法层面上的调查及裁量判定问题，而不属于传统审计的问题领域与对象范围。

但是，作为一种重要而独特的监督治理手段[①]，审计制度的领域范围不是僵化不变的，而是会随着时代的发展要求而不断变化拓展。例如，2018年8月，审计署发布《关于进一步加强减税降费政策措施落实情况审计监督的意见》，要求对税收经济政策的遵从合规情况进行审计监督。2018年12月，审计署发布《关于加强信息系统审计工作指导意见》，要求对信息系统的安全性、可靠性和经济性进行监督检查，推动完善相关制度，促进提高资金使用绩效，保障信息系统安全、可靠和高效运行。2019年《关于实行审计全覆盖的实施意见》等政策出台后，自然资源的开发利用与环境保护进一步成为审计制度的新领域。2023年5月23日，习近平总书记在二十届中央审计委员会第一次会议上发表讲话时指出，要加大关于稳经济、金融支持实体经济等宏观政策的落实情况的审计力度。上述变化表明，在对经济活动本身进行审计监督外，审计制度进一步拓展到与经济活动及公共受托责任相关的各种问题领域，如经济政策的遵从落实问题。在数字及人工智能化时代，审计制度进一步延伸拓展到个人信息保护合规领域是时代发展的需要，个人信息保护合规审计旨在鉴证个人信息处理行为是否符合既定标准，是合规审计覆盖范围与功能作用的进一步延伸和扩张（陈智敏，2022）。个人信息保护合规审计能够有效弥补监管部门的资源紧张，是信息保护合规监管的有效补充（王俊等，2023）。本文认为，合规审计不仅为个人信息保护的合规监管与治理提供了有效抓手与支撑，而且其本身也构成了信息保护合规监管与治理的重要内容与功能模块。目前，个人信息保护合规审计已经成为国际通行的

做法，在数字中国建设的大背景下，开展个人信息保护合规审计具有重要的实践意义（高歌，2023）。为此，应充分遵循和运用合规审计制度特有的分析审查视角、功能逻辑、运作路径、技术方法，着眼于个人信息保护的风险识别与合规治理体系建设和能力提升等综合目标，逐步创新建构和运作个人信息保护合规审计的各种制度和相关方法。

2. 确保数据资源合理利用及数字经济健康发展的底层逻辑。在继劳动力、土地、资本、技术等基本的生产要素之后，数据资源已成为数字经济时代最重要的新的生产要素，也是中国经济在新时代高质量发展的重要驱动要素。2022年12月，中共中央、国务院发布《关于构建数据基础制度更好发挥数据要素作用的意见》（简称《意见》）。在建立数据要素的流通、交易及治理制度方面，《意见》要求培育合规认证、安全审计、数据公证等第三方专业服务机构；建立数据要素生产流通使用全过程的合规公证、安全审查、算法审查、监测预警等制度，指导各方履行数据要素流通安全责任和义务。显然，为充分保障和发挥数据要素资源的作用，《意见》要求建立安全审查、合规监管等重要基础制度。由于个人信息是数据资源的重要来源和形成基础，因此，如何充分保护个人信息权益，确保公平合理、合法有序地搜集处理、开发利用个人信息数据关系到数据资源可持续的合理开发利用，进而关系到数字经济的可持续发展。对个人信息的适度收集和合理利用是数字经济发展的逻辑前提。在我国，个人信息保护有助于保障我国数据要素市场的规范基础及其健康发展。从全球经济的竞争发展来看，涉及个人信息的数据开发利用日益成为全球数字经济竞争发展的原动力，个人信息保护将为我国参与全球数字经济竞争发展提供有效保障（黄哲瑞和徐来凤，2023）。因此，一方面，从宏观经济层面看，个人信息保护不再仅仅只是私人权益保护的问题，而是事关社会经济健康运行、和谐发展的重要问题之一；另一方面，从微观经济层面看，个人信息保护是数字经济时代企业参与市场经济活动，在经营发展上“行稳致远”的重要要求和保障。作为评价、监督经济生活运行与微观经济活动的专门机制和工具方法，审计自然可以也应当介入个人信息保护领域，并通过其功能的拓展与创新充分发挥其在新领域的评价和监督作用。

二、合规审计的“裁量判断”强属性及应遵循原则

（一）信息保护规则的抽象性及合规解释裁量的强属性

对个人信息保护进行合规审计需要以明确、具体的信息保护义务、行为标准等为基础依据和参照，但是，面对不断更新变化的算法技术和数据信息开发利用的复杂多样的市场需求与活动，个人信息保护的各种义务规则往往只能是一种高度概括性的抽象规定，即便在某些方面也可能形成较为具体的行为义务规则或标准，但仍然可能不足以适应各种具体情况。这就需要审计人员根据具体的个案情况，对概括抽象的个人信息保护规则做出精准、恰当的具体解释。这就意味着，与关于财务收支、经济绩效等问题的审计监督不同，个人信息保护的合规审计具有强烈的规则解释适用上的“裁量判断”属性。鉴于规则解释适用上所固有的复杂性、灵活性、多元性、开放性等，合规审计上的“裁量判断”将面临明显的障碍与困难。为此，笔者结合个人信息保护的相关规则做适当举例分析。

1. 对各种情形下的“必需”条件的衡量判断。根据《个人信息保护法》第十三条，属于该条第一款第（二）项至第（七）项所规定情形的，处理、利用个人信息不需取得个人同意。如第一款第（二）项所规定的“为订立、履行合同所必需”；第一款第（三）项所规定的“为履行法定职责、义务所必需”；第一款第（四）项所规定的“为应对突发公共卫生事件等所必需”等。但是，如何判断上述各种情形下的“必需”，法律并未明确规定，在合规审计时如何做出准确、恰当的裁量判断就必然面临着困难与不确定性。

2. 对“有效的告知”的衡量判断。《个人信息保护法》确立了以“告知—同意”为核心的个人信息保护的合规原则，《个人信息保护法》第十七条规定对“有效的告知”提出了具体要求。2023年发布的《个人信息保护合规审计参考要点》对“有效的告知”提出的进一步要求是，告知文本的大小、字体和颜色应便于个人阅读认知等。即便如此，这些似乎较为具体的各种要求仍然需要进一步的解释明确，如是否达到“显著、真实、准确、完整”这些要求，是否已经构成“有效的告知”，仍然需要合规审计人员在个案中做出具体的裁量判断。

3. 对“敏感个人信息”的衡量判断。《个人信息保护法》通过设置第二节共五个条款，对“敏感个人信息”的处理提出了特殊规制要求。其中，第二十八条第一款采用“概括+列举”模式界定了何谓“敏感个人信息”，该类信息首先被抽象概括地界定为“一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息”，然后，具体列举了七类典型的敏感个人信息。但是，王苑（2022）指出，这样的界定可能带来如下的不确定性：（1）法律评价标准具有模糊性；（2）未来会出现的新的敏感个人信息不在具体列举的范围；（3）判断标准的多维性导致分析确定的困难。对此，应通过综合考量五个方面的要素，动态界定敏感个人信息。因此，如何区分“敏感个人信息”与“非敏感个人信息”，需要合规审计人员根据具体的个案情况做出动态的解释裁量判断。

4. 对“特定的互联网平台”的衡量判断。《个人信息保护法》第五十八条提出了“守门人”条款，对符合特定条件

的互联网平台施加了特别的信息保护义务。但是，有学者分析指出，“守门人”条款的规定过于简略，该条款究竟如何理解与适用，存在不少问题和争论，需要进一步解释明确。例如，对于某个互联网平台是否属于“守门人”，第五十八条提出了“提供重要服务、用户数量巨大、业务类型复杂”这三个叠加条件。这意味着，确立了“先分类、再分级”的识别判断标准。“提供重要服务”意味着要先对平台服务进行分类，“用户数量巨大、业务类型复杂”意味着在分类的基础上再根据这两个标准对平台企业进行分级，最终识别确定某互联网平台是否属于“守门人”（周汉华，2022）。然而，对于这些识别判断的环节和要求，缺乏明确细化的解释、指导。对此，合规审计人员需要根据用户规模、业务类型、经济规模、信息数据的利用程度等在个案中做出具体的裁量判断。

（二）合规裁量判断应遵循的指导原则

为应对解决合规审计中“规则解释适用”上的障碍与困难，精准、恰当地裁量判断个人信息保护合规状况及风险问题，应当确立和运用各种指导原则。这些原则主要包括：合规审计裁量权的审慎运用原则；利益衡量上的比例原则；合规审计的裁量基准原则；体系解释原则；审计独立下的沟通及共识解释原则。本文仅就其中的两个原则做进一步的分析阐述。

1. 利益衡量上的比例原则。在个人信息的收集处理及加工利用活动中，个人的信息权益保护实际上是一个各方利益协调平衡的问题。就信息处理者而言，它们包括立法机关、司法机关、政府部门、企业以及其他社会组织等。国家机关、政府部门在收集处理及加工利用个人信息时，行使的是公权力，代表和体现了国家利益、社会利益；而企业和其他社会组织在收集处理及加工利用个人信息时，代表和体现的是企业和其他社会组织自身的经济利益或其他利益。就作为信息来源的个人而言，他们对自身的信息享有充分的身份权益和经济权益。显然，信息处理者与作为信息来源的个人有着各自独立的利益归属与诉求，双方的利益有时是协调一致的，有时则是相互矛盾冲突的。梁灯（2022）分析指出，特别是在企业作为个人信息处理者时，将面临着个人信息的价值挖掘和个人信息权益保护之间的冲突和平衡问题，当个人数据信息在企业间流转时该问题最为凸显。因此，在个人信息保护合规审计中，对相关规则的解释适用往往所涉及的是相关主体的利益得失问题，所谓的合规判断也就是根据抽象规则对相互矛盾冲突的利益进行衡量平衡处理。显然，如何对各方利益进行合规裁量上的协调平衡，需要形成和运用相应的指导原则。对此，本文认为，可以参考借鉴行政法上的比例原则，在个人信息保护合规审计制度中，塑造形成关于规则解释适用的利益衡量比例原则。

比例原则是行政法上的一个重要原则，它被用于约束规制行政权的自由裁量行使，谋求在行政目的、需要与相对人的利益保护之间实现协调平衡。其基本要求是，行政主体实施行政行为应兼顾行政目标的实现和保护相对人的权益，如果行政目标的实现可能对相对人的权益造成不利影响，则这种不利影响应被限制在尽可能小的范围和限度之内。行政法中的比例原则包含适当性、必要性和相称性（均衡性）的多维度内涵。适当性又称为妥当性、妥适性、适合性，是指所采取的措施应当能够或至少有助于实现行政目的。必要性又称为最少侵害性、不可替代性。即在能实现行政目的的多个方式中，应选择对权利影响或侵害最小的方式。相称性也称为均衡性，即行政措施与其所达到的目的之间必须成比例或相称。相称性（均衡性）侧重要求的是，无论是否存在多个可选择的措施、方法，行政措施不能过分地或不适当地影响、损害相对人的合法权益。笔者认为，在个人信息保护方面，信息处理者与作为信息来源的个人在相互地位关系及利益结构上非常类似于行政机构与相对人之间的关系，尤其是信息处理者为国家立法、司法机关、政府部门时更是如此。因此，应当参照行政法上的比例原则，按照对个人造成最少最小影响的原则来解释适用个人信息保护的相关规则，以矫正个人在信息的收集处理及加工利用中的弱势地位，充分保护个人对自身的信息所应享有的身份权益和经济权益。实际上，在个人信息权益保护上，利益衡量上的比例原则在立法上已经有所体现。例如，《个人信息保护法》第六条规定，处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息时应当限于实现处理目的的最小范围，不得过度收集个人信息。显然，该条所提出的要求已经基本上体现了比例原则所包含的适当性、必要性和相称性（均衡性）要求。

需要指出的是，一般而言，根据合规裁量上的比例原则，应采取对个人造成最少、最小影响的方式来解释适用个人信息保护的相关规则，但是这不是绝对的。当信息处理者投入大量的资金等成本对个人信息进行深入加工并已经形成稳定的、明确的商业利益时，信息处理者将获得一种独立于个人权益的“既得权益”。2023年12月财政部制定发布的《关于加强数据资产管理的指导意见》明确规定了数据开发利用者基于其投入付出及再创造应享有的独立的受益权②。此时，就不能简单按照对个人造成最少、最小影响的方式来解释适用合规裁量上的比例原则，而应当以兼顾平衡的方式来运用比例原则。例如，《个人信息保护法》第十五条规定，基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。显然，

如果信息处理者已经投入成本加工处理个人信息的，或者进一步将其予以商业共享或转让的，无条件地允许个人撤回同意则可能损害信息处理者的商业利益。对此，仅仅确认“撤回前基于个人同意已进行的个人信息处理活动的效力”是不够的，应当根据比例原则中的“兼顾既得商业权益”的要求，充分考量撤回同意的必要性，以利益平衡的方式分析评估撤回同意的合规性问题。

2. 审计独立下的沟通及共识解释原则。鉴于个人信息保护规则具有高度概括抽象性，审计机构和人员需要对相关规则进行解释，这就会造成各方对同一规则的不同理解和判断。对此，审计机构和人员可以与被审计企业及监管部门等进行沟通形成共识理解。但是，有研究认为这可能会导致审计独立性及权威受损。例如，由被审计单位委托进行合规审计时，受托审计机构在沟通交流中容易受委托方的影响，从而对信息保护规则做出有利于委托方商业模式的解释和定性判断。在监管部门所要求启动的审计中，外部审计机构往往需要与监管机构进行沟通交流，从而会受到监管机构立场的影响，做出不利于被审计方的分析评价（梁灯，2022）。

笔者认为，鉴于个人信息保护规则的高度概括抽象性以及个人信息开发利用的复杂多样性，在合规审计中寻求沟通并形成共识解释将是一种常态现象，寻求沟通形成深入、准确的了解判断也是审计工作中的常规做法。现有的一些审计准则也有进行沟通形成共识的要求，如2013年中国内部审计协会制定发布的《第2105号内部审计具体准则——结果沟通》。同时，寻求沟通并形成共识解释并不必然损害合规审计的独立性和权威性，或者说，寻求沟通并形成共识解释并不是合规审计的独立性和权威性受影响的真正原因。在寻求沟通并形成共识解释中，合规审计不能维持其独立性和权威性的重要原因在于，审计人员缺乏对相关规则的深入理解把握，没有形成坚实的合规审计上的衡量判断能力。在个人信息保护的合规审计中，面对相关规则的概括抽象性及解释适用，寻求沟通并形成共识解释将有助于审计人员更加全面深入地理解规则的内涵及被审计的具体情况，并形成高质量的合规审计结论。因此，在不断提升审计人员的规则解释及衡量判断能力的基础上，将能够也应该确立审计独立下的沟通及共识解释原则。

三、个人信息保护合规审计的框架及方法的建构运作

个人信息保护的合规审计应当立足于“调查分析”“监督问责”“风险防控”“督促整改”等专门视角与特有功能，逐步建立完善相关的审计框架、功能模块、指标体系、技术方法等，以形成一个综合全面、立体多维、契合紧密、功能卓越的合规审计制度与机制。本文就其中的若干方面进行适当的探索分析。

（一）确立定性与定量分析相结合的框架方法

个人信息保护合规审计的定性分析是一种符合性评价，即对处理个人信息的行为和活动是否符合法律规定做出肯定性或否定性的审计评价。这是个人信息保护合规审计的基本内容和结论要求。在此基础上，个人信息保护合规审计还应进行定量分析，即对个人信息处理的行为和活动偏离法律规则的程度进行量化界定，并建立和运用量化评估的赋值指标体系。对行为的偏差度的量化分析具有重要的价值和作用。“合规偏差度”的量化分析评价可以精确、具体地揭示个人信息处理及利用的合规状况，进一步确定各种偏差所造成的不同危害及应采取的纠正措施，进一步分析判断不同的偏差样态造成的危害风险并进行预警。进而言之，“合规偏差度”的量化分析评价有助于开展“审计容错纠错”的实践。对于个人信息保护合规审计而言，“合规偏差度”下的“审计容错纠错”将解决两个维度的问题。一是关于个人信息保护的规则尤其是较低层级的具体规则存在着错误、不当、不合理之处，或者过于僵化、教条，对此，需要运用“合规偏差度”的量化分析评价，通过“审计容错纠错”的方式予以解决。二是关于个人信息保护的规则存在着滞后性，不能充分适应信息开发利用和信息保护中的各种新情况与新问题，对此，需要运用“合规偏差度”的量化分析评价，通过“审计容错纠错”的方式予以解决。当然，在审计容错纠错中，对于触及法律法规底线的问题，绝不能以容错纠错之名予以放纵（项健，2021）。

（二）建立模块化的审计框架与指标体系

模块化的审计框架是指根据多样化的审计目标设置不同的审计模块单元。在模块单元下，可以进一步细化具体的审计事项与指标等。例如，就算法审计这个特定目标而言，可将审计框架划分为“总体风险控制与治理”与“过程风险控制与治理”两个模块。总体风险控制与治理模块所针对的是算法设计及风险治理的制度框架，例如是否成立算法风险治理领导小组、是否存在算法设计和运行的合规审查制度等；过程风险控制与治理模块所针对的是算法系统在运作过程中的问题与风险（张欣和宋雨鑫，2022）。本文认为，模块化的审计框架意味着，个人信息保护的合规审计并不仅仅只是对信息处理和利用的行为或活动本身的合规性进行审计分析评价，而是将个人信息保护看作是一项全方位的系统工程，是从宏观框架到微观环节进行多维的综合审计分析评价。因此，对于个人信息保护的合规审计，应当根据个案所要求的不同的审查视角与目标设置模块化的审计框架，既包括个人信息保护在总体架构层面的合规审查模块，也包括在个人信息处理过程中各个环节及问题的合规审查模块，从而形成综合全面、立体多维的合规审计分析评价。

（三）建立信息处理系统功能设计的合规审计制度

在关于个人信息的隐私保护方面，一些国家已经形成“通过设计的隐私保护”（Privacy by Design）和“隐私工程”（Privacy Engineering）这两个不同的保护环节。这就意味着，个人信息隐私保护包含着两个不同的阶段，即系统功能（算法）设计阶段与个人信息处理阶段的个人信息隐私保护（William Stallings，2019）。本文认为，个人信息权益保护的内容范围显然要大于个人信息的隐私保护，但同样也存在着系统功能（算法）设计阶段的保护与个人信息处理阶段的保护这两个不同阶段的个人信息保护。一般而言，通过对个人信息处理阶段的合规审计，也可以间接发现系统功能（算法）设计上的保护缺陷，但是这种暴露往往是不充分和滞后的。因此，为充分揭示和有效预防控制个人信息保护上的缺陷及风险，应当建立专门针对信息处理系统的功能（算法）设计的合规审计。在这方面，已经形成了一些重要准则和指南，如中国内部审计协会于2014年制定发布的《内部审计具体准则——信息系统审计》，于2021年制定发布的《内部审计实务指南——信息系统审计》，以及2018年12月审计署发布的《关于加强信息系统审计工作指导意见》。

（四）建立信息处理过程的合规风险持续控制制度

由于个人信息的收集处理与开发利用具有技术复杂性、隐匿性及数量庞大性等特点，所以，运用传统审计思路与方式进行合规审计往往难以产生良好的预期效果，因此，有研究认为，应建立和运用CRCA模型（持续性风险评估与控制保证模型）来开展个人信息保护合规审计（陈智敏，2022）。显然，合规风险持续控制分析侧重关注的是个人信息保护风险的及时、准确识别，以及将持续处理过程中的风险动态变化置于监控之下，这有助于在信息处理持续过程中实现对个人信息权益的动态及时保护。但是，《个人信息保护合规审计管理办法（征求意见稿）》只是提出了一定年限内的单次合规审计要求，并没有提出关于“合规风险持续控制分析”的要求。例如，对于处理超过100万个人信息的信息处理者，仅要求每年至少应实施一次合规审计，其他情形下则要求每两年至少应实施一次合规审计。因此，需要在该征求意见稿中补充纳入“合规风险持续控制分析”的要求。

四、结语

个人信息保护合规审计是合规审计制度在数字及人工智能时代的新拓展，是个人信息保护的合规监管与治理的有效抓手与重要内容。但是，个人信息保护合规审计制度尚处于初步建立阶段，相关的理论问题与操作实施尚处于探索中。笔者就个人信息保护合规审计制度的底层法理逻辑、特征属性、功能需求、指导原则等理论问题进行了初步探讨，更多的和更深层次的理论问题需要进一步分析研究，如个人信息保护合规审计的性质类型及其与国家审计的衔接协调，合规审计中关于“合规”要求的渊源依据等。同时，需要深入、全面地分析研究个人信息保护中的各种案例和实际问题，针对个人信息保护合规审计制度，进一步分析建立和调整完善该领域特有的工具方法、程序规范、功能机制等。

【注　释】

①党的十九大报告将审计放在“健全党和国家监督体系”部分予以阐述。党的十九届四中全会明确提出审计监督是党和国家监督体系的重要组成部分。

②《关于加强数据资产管理的指导意见》将“畅通数据资产收益分配机制”作为数据资产管理的一项主要任务。针对完善数据资产收益分配与再分配机制，该指导意见要求按照“谁投入、谁贡献、谁受益”的原则，依法依规维护各相关主体数据资产权益。支持合法合规对数据资产价值进行再次开发挖掘，尊重数据资产价值再创造、再分配，支持数据资产使用权利各个环节的投入有相应回报。

【主要参考文献】

陈智敏.个人信息保护合规审计系统构建研究[J].审计观察，2022(12)：18～22.

高歌.个人信息保护合规审计蓄势待发[N].中国会计报，2023-09-01.

黄哲瑞，徐来凤.个人信息保护法对我国数字经济发展的重要价值[N].科学导报，2023-10-17.

贾丹，张誉馨，王姗.我国个人信息保护合规审计制度的路径探讨[J].工业信息安全，2022(4)：17～22.

梁灯.个人信息保护合规审计的悖论及其解决——以个人信息流转合法性基础为例[J].上海法学研究(集刊)，2022(20)：84～93.

刘力云，崔孟修，王慧，沈玲.对国家审计基本概念仍需深入研究——基于一项有关国家审计基本概念和定义认知访谈结果的分析[J].会计之友，2021(8)：15～21.

王苑.敏感个人信息的概念界定与要素判断——以《个人信息保护法》第28条为中心[J].环球法律评论，2022(2)：85～99.

王俊，冯恋阁，钟雨欣，郑雪.网信办拟细化个人信息保护合规审计，企业需定期做“体检”[N].21世纪经济报道，2023-08-04.

项健.审计容错纠错思维方式探讨[J].审计月刊，2021(10)：23～24.

周汉华.《个人信息保护法》“守门人条款”解析[J].法律科学，2022(5)：36～49.

张欣，宋雨鑫.算法审计的制度逻辑和本土化构建[J].郑州大学学报(哲学社会科学版)，2022(6)：33～42.

William Stallings. Information Privacy Engineering and Privacy by Design：Understanding Privacy Threats，Technology，and Regulations Based on Standards and Best Practices[M]. New York：Addison Wesley，2019.

（责任编辑·校对：刘钰莹　罗萍）