DOI: 10.11817/j.issn. 1672-3104. 2022. 03. 003

公共卫生领域大数据治理中个人信息的利用与保护

许中缘，何舒岑

(中南大学法学院，湖南长沙，410006)

摘要：个人信息是公共卫生领域大数据治理中的核心要素。我国公共卫生数据治理存在个人信息私密性与公共性价值冲突的平衡难题、多元治理主体间的信息整合困境及个人信息利益建构性损害的救济障碍。公共卫生领域相关法律规范在大数据治理和个人信息保护规则方面的滞后性，是阻碍数据利用效能、削弱权益保护的表层原因，个人隐私保护与公共健康保障的价值矛盾是冲突根源。限制个人信息私利性，应以保障公共卫生安全为法定依据和价值基础，遵循基于场景解构的差异化、动态化合规处理规则及具备可救济性的限度要求；应对相关法律规范加以完善，具体包括细化个人信息差别化公开和共享规则，厘清多元主体权责配置，加强个人信息权益行政监督与救济。

关键词：公共卫生；大数据治理；敏感个人信息；利益冲突；场景理论

中图分类号：D923.8 **文献标识码**：A **文章编号**：1672-3104(2022)03−0020−12

公共卫生领域被视为大数据技术应用中前景最好的领域之一。目前各国理论和立法存在对“信息”与“数据”用词交互使用的现象[1]。数据通常被理解为个人信息表达的载体形式之一，在这个意义上，二者内涵具有天然的共生性与一致性[2]。但在数据治理研究领域，更多观点认为信息的外延大于数据，个人信息因其涵盖的内容而具有更多意义[3]。鉴于此，个人信息也是公共卫生领域大数据治理中特殊的核心要素。公共卫生领域相关个人信息主要由健康医疗数据组成，还包括部分个人网络行为、生活习惯、行踪轨迹及身份信息等，这些个体关联信息共同构成了公共卫生治理体系数据库的内容。其中，健康医疗数据是涉及权利主体最多也最敏感的数据类型之一[4]。从公共卫生大数据治理视角看个人信息利用与保护问题，表面上是对数据治理机制的探讨，其实也是对具有识别性的相关敏感个人信息处理规则的研究。

相比传统管理方式，通过物联网、大数据、人工智能等手段进行信息处理的现代化治理方式①，在预防和预控公共卫生危机方面能产生更大的社会公共效益[5]。我国《民法典》、《刑法》修正案和《个人信息保护法》在一定程度上已增强了公共卫生数据治理中个人信息保护的制度保障。但实践中，在信息的收集、存储、流转、加工和使用等不同阶段，除了治理机制效率及其有效性体现不足之外，还存在个人信息不当泄露、收集或滥用等侵害风险，以及因信息处理规则不完善造成的社会歧视、公众恐慌等社会风险，甚至是国家信息安全风险。究其原因，是当前我国公共卫生数据治理机制在规范安排上尚呈现零散化样态，数据治理理念和具体实施规则存在滞后性②，也未充分凸显公共卫生领域个人信息处理的特殊性。现行网格化公共卫生管理机制缺乏对个人信息处理行为的规范区分，由此产生了主体权责混乱及信息控制失灵的困境[6]。

基于此，本文将从公共卫生领域个人信息利用规制存在的现实问题出发，从规范层面挖掘问

收稿日期：2022−01−11；**修回日期**：2022−04−06

基金项目：湖南省研究生科研创新项目“大数据时代企业数据权益的立法保护研究”(CX20200378)

作者简介：许中缘，男，湖南武冈人，法学博士，中南大学法学院教授、博士生导师，中南大学卫生法研究中心主任，主要研究方向：民商法、卫生法学等；何舒岑，女，湖南长沙人，中南大学法学院博士研究生，主要研究方向：卫生法学、数据法学，联系邮箱：499501407@qq.com

题产生的原因，并围绕个人信息公共性和私益性之间的价值冲突，探索理论层面的制度根源，拟为我国公共卫生数据治理中个人信息利用与保护相关规范的进一步完善提出建议。

一、公共卫生大数据治理中个人信息利用规制存在的问题

(一) 个人信息私密性与公共性的价值冲突

在大数据治理背景下，个人信息不仅涉及个人利益，而且关涉他人和整个社会利益，具有公共性和社会性[7]。但相对而言，公共卫生领域个人信息的内容范围更广，隐私性、敏感性比其他领域更强。个人信息本质上的矛盾在公共卫生数据治理机制运行中尤为凸显，实践中的价值冲突也未得到妥善解决。

一是个人信息的保密性与公开性。对于公共卫生领域相关个人信息公开或保密的界定标准，不同主体因职责或理念不同而难以达成一致。例如，对于通报制度，公共卫生行政部门认为其首要职责在于保护公众利益，以集体利益和科学伦理的视角来表达医疗机构或医生的通报义务之正当性，必要信息通报也应当公开透明；多数医学机构或患者则认为，维护病人个体之隐私利益应被视为首要任务，个人医疗信息应被保密[8]。同时，公共卫生领域敏感个人信息的私密程度，于不同人群的内心感受而言存在差别，相关信息组成也有其多样性和复杂性，使得该领域难以完全适用现行相关法律规范中原则性较强的统一标准。信息类型化研究与公开标准细则的缺失，使公民对于涉隐私的保密要求与社会对于涉公共安全的公开需求之间的冲突，难以充分化解，也加深了实际工作中的判断难度。在治理实践中，相关人员难以把握个人信息保密性与公开性的界限，会导致对公开信息的利用未能落实，对保密信息的保护也不到位。

二是个人信息的隐私性和共享性。大数据治理主要基于预判模式，治理成效与数据的数量和质量关联性较大。打破行业信息共享限制，实现跨部门、跨主体数据融通，有助于扩大样本量、保障内容有效性和真实性，促进实时动态分析、提升机制效率和决策准确性。然而，个人信息双重性质的矛盾，也使公共卫生数据的共享要求遭遇了挑战。一方面，在当前常态化公共卫生规制中，不同部门间客观上普遍存在“信息孤岛”现象，数据共享不充分③。另一方面，实现数据共享意味着个人信息会在不同主体间流转、处理和利用，在缺乏数据权属认定和完善的共享规范的情形下，易造成共享不足、权责混乱、主体行为标准不统一等问题。在个人收益和公共收益并存的前提下，为了某领域公共卫生项目或议程的推进，如疫苗接种计划的推行，会因信息数据共享、开放和流转不规范而导致个体隐私被侵害，甚至引发社会秩序混乱或歧视等问题。此外，新主体通过算法加工会挖掘出新的信息，产生二次个体关联性，即使是匿名化后的个人信息在二次加工与流转过程中仍存在可识别风险，而相关规范缺失对二次共享行为的脱敏处理规则。

(二) 大数据治理信息整合的主体多元

大数据技术推进多元信息控制主体成了共同治理主体，数据利益攸关者之间需相互积极回应，铸就相互依赖关系、共同发掘数据价值的基础性架构[9]。公共卫生信息化规制的成效，很大程度上取决于公众和相关参与主体对行动的整体回应。但如今数据生产者与数据控制者相分离，数据被不同主体交叉持有成为一种常态[10]。而公共卫生领域个人信息具有更鲜明的基层属性，通常被分散控制于政府、医疗机构、疾控中心、高校、企业及其他社会组织等不同主体之中。相关信息的类型复杂多样、来源广泛且分散，使共治实践中存在信息整合困境。同时，多元主体对个人信息的利用规制行为还存在融合度和回应度不高等问题，未能充分发挥各自优势，进一步限制了信息资源的整合。

首先，政府主体监督力和领导力体现不足。共治模式需要有强监督，如我国《传染病防治法》第 5 条确认了由各级人民政府领导传染病防治工作，将“依靠群众”作为防治原则。在日常公共卫生行政工作中，这一结构行之有效，在将基础原则落实到数据治理中时，却略显不足。一方面，在应对风险时，国家是传统的权威统计和领导组织，但在新技术应用和共治要求面前，技术平台

和社会组织运用大数据的能力远超传统国家的统计功能[11]。大数据治理实践水平在整体上呈现城乡、区域、行业间的失衡，增加了地方政府指导的难度。另一方面，对政府在信息处理上的主体责任存在认知与规范欠缺。公共卫生规制强调政府主体时，宜以“政府整体”代入治理进路，而当前规范和实践中大多限定于有特定权限、依授权就卫生问题展开行动的主体，如卫计委或特定岗位官员[12]。若焦点置于特定行政分支，反而凸显特定主体的权责，削弱整体领导力。当技术环境和治理环境发生变化，如果公权力运行状态和相关规范均未能迅速作出更新回应，则治理实效和信息安全会受到影响。

其次，社会组织主动性与积极性体现不足。北京市的调研发现，疫情期间，48.21%的相关社会组织因“没有资金支持”“不知道做什么”“找不到服务对象”等原因完全未参与防控工作[13]。部分社会组织除了客观上受限于医疗专业知识水平，主观上也倾向于依赖行政部门为其提供行动框架以规避风险，且认为自身参与日常监测或特定防控工作缺乏直接关联和义务，因而较为懈怠和被动。事实上，各类社会组织掌握了大量个人信息，其主动参与大数据整合与治理将产生积极作用。例如，数字企业拥有强大的数据资源采集和加工能力，行业组织具有较高信息更新速度，媒体在一定范围内能推进有效信息的发布与传播等。社会组织在法定范围内，若能主动、及时地向行政主体归集相关原始信息或加工信息，可以丰富数据类型，扩大渠道，推进信息整合。

最后，医学专业主体能动性和独立性体现不足。疾控机构、医学专业机构、医学院校及其专业人员等，对于公共卫生领域相关信息的认知和把控强于其他主体。然而，政府或卫生行政部门往往享有治理决策的主导权，一般不直接收集、处理一手个人信息，而疾控机构能及时掌握并处理信息，规范上却没有凸显其能动优势与独立地位。在此配置下，数据治理会相对缺少科学因素的介入而影响决策理性。一方面，由于医疗数据专业性强，若缺乏有效转化和处理的途径，将难以被作为常识性数据加以利用，从而限制大数据应用的范围和效率，或造成决策者难以及时整合有效信息。另一方面，部分官员因受主观偏好和个人动机的影响，存在隐瞒和谎报信息的行为，缺少疾控机构独立性监督的介入，可能影响信息公开或决策的准确性，引发信息失真或流通折扣等问题[14]。

(三) 个人信息建构性损害的救济失范

在环境污染、公共卫生等领域，侵害行为往往不会在当下对他人造成明显的损害，或造成难以发现的损害，但会使他人将来因此受到损害或增加受损害的可能性，进而导致社会力量的失衡，产生或加重损害结果，有学者称之为“建构性”损害[15]。例如，基于行政主体对个人信息的滥用而产生的疫苗分配不平等、对吸烟酗酒人群的社会歧视，或难以确定突发性公共卫生事件风险程度时对个人信息所作的不恰当处理等。面对公共卫生领域个人信息的公共性、交叉性和损害建构性等特点，现有救济规范针对性不足。

首先，公共卫生领域个人信息侵害的私法诉讼路径效果有限。当前我国个人信息的法律治理路径主要通过“告知—同意”机制来实现，对个人信息保护偏重于民事或刑事诉讼救济，行政救济路径相对缺失[16]。而实践中公共事项治理领域的信息侵害又常常存在私法追责困境。一是当前“数据治理”作为提升行政效率和管理效能的政府管理新方向，开始被要求从国家权力运作和公共管理角度对相关工作进行整体审视和追责[17]。个别诉讼形式难以有效回应系统性社会风险治理与责任问题。二是个人信息一旦被以数据化形式存储，就大多被掌握在政府、科研机构及商业组织等不同数据库中，如缺乏有效行政救济，基于主体实力和地位不平等、诉讼成本高和信息不对称等原因，个人很难实现对专业数据处理行为的维权[18]。

其次，个人信息侵权损害的识别与认定难。在司法实践中，个人信息被侵害通过私法维权时，常因理论难点或技术认定上的障碍，较难获得法院支持。如 2017 年 1 月至 2019 年 9 月公开的数据维权案 12 件，其中 9 件维权失败，主要原因在于用户无法完成举证责任[19]。《个人信息保护法》出台后，明确了侵权的过错推定原则，

适当回应了举证难的问题，从诉讼与程序规范方面加强了个人信息维权保障力度。然而，基于公共卫生领域的特殊性，对于相关利益的损害识别、损害举证和司法认定仍存在难题。具体来说，“无损害，无救济”彰显了损害在救济制度中的核心地位[20]。在损害理念影响下，民众倾向于在实体权利受到侵害后才寻求司法救济，而不是在察觉到存在侵害危机的当下即寻求救济。但一方面，相比洪涝、气象、泥石流等自然灾害风险治理机制，公共卫生治理过程的阶梯性更明显、持续期间更长、治理技术与手段更复杂，尤其在面对新发疾病时，风险判断和利益损害的不确定性大。由于风险起始时点模糊，个人司法维权难以追溯事前。而对于事后因滥用公共利益理由而侵犯个人信息等情形，造成损害后果，难以用证据证明。另一方面，相比交通、金融等数据治理领域主要基于历史数据和经验进行判断，公共卫生治理决策因新发问题较多而更注重相关关系预判模式，不确定性更强，预判结果大多属于经验或概率上的结论。公共卫生规制存在难以避免的“决策于未知性之中”的困难，即在作出决策的紧急关头，很难确认当下采取的特定措施会被后来者评价为反应过度还是不足[21]，甚至在遭遇个人信息利益被侵害后的一段时间，个人也意识不到侵害的存在。

总的来说，对于领域内的“建构性”损害，司法认定在技术认知、概念理解和规范选择方面仍存在一定障碍，侵权法也只能为公共卫生领域提供有限的助益，个人权利救济门槛较高。

二、公共卫生数据治理中个人信息利用规制问题产生的原因

(一) 个人信息处理行为的规范模糊阻碍机制运作

将个人信息作为纯粹私权的保护路径，可能产生信息价值密度低、智能处理程度弱、信息获得与使用结果间相关性弱等问题[22]。基于公共利益需求，公民需对个人信息隐秘性和自主性适度放松或让位。因为通过信息环境的改变，能促进社会作出更有益于群体利益的选择，有利于提高数据的公共价值。但让位与保护行为之间的界限需被进一步明晰，在数据治理机制的实际运作过程中，关于个人信息双重性质上的现实冲突才能得以缓解。

首先，公共卫生领域个人信息公开性与保密性的界定标准缺乏操作性强的规范细则。例如，针对疫情期间，规范上未明确限定允许采集区域内或途经人员信息的主体，信息通报和公开的内容范围及条件也未有效规范；针对日常规制，缺少可公开和禁止公开个人信息的界定标准及其认定主体等规范内容。同时，我国涉及隐私的信息公开相关规范与个人私密信息保护规则的不一致，也会造成边界认定的混乱。如我国《政府信息公开条例》把对政府信息是否涉及个人隐私、公开是否会侵害第三人权益或对公共利益造成重大损害、权利人不同意公开的理由是否合理等内容的判断权，过于宽泛地授予行政机关裁量行使，这与隐私权的法律保留原则相悖[23]。

其次，个人信息共享与开放规范不够完善。现有数据开放共享规范，层级和效力普遍不高，且相关实施细则的原则性条款较多，未能明确公私主体间信息共享的内容范围、条件和方式等。如《国家健康医疗大数据标准、安全和服务管理办法(试行)》，旨在保障公民知情权、使用权和隐私权的基础上，规范医疗数据的开发。但其并没有在限定主体范围、数据流转、利用和保护方面提出具体操作规则，只有一般化的基本原则和要求，对于个人信息再利用的匿名化保护规范也存在缺失。这不仅导致重要数据流通和利用渠道不畅，制约个人信息公共性利用效率和治理效能，也可能使治理主体在实践中因缺乏信息获取和共享的依据而畏首畏尾，影响多元联动。

(二) 多元信息主体权责配置不明制约治理响应

在高度不确定性的公共卫生风险治理情境下，基于大数据多重检验的理性决策，能适当避免自发性行动犯错的可能性。治理的基础不是控制而是协同，是多元权力(权利)的持续互动、信任合作与协调平衡[24]。当多元共治要求结合数字化背景时，相关治理产生了信息整合困境、主体权利冲突和联动回应不足等问题，主要原因是规

范上未能厘清不同信息主体的制度定位与分工并合理协调多元主体的权责义配置。

首先，就政府主体而言，除了平台建设、技术人才、数据能力等客观条件略有欠缺的原因外，还在于现有规范未确认其在公共卫生领域对个人信息利用规制的领导与监督方面的责任主体地位，没有突出保障权责统一的实现。不论是个人信息保护法还是公共卫生法律规范，均未设定对个人信息侵害行为的专门行政监管机构。同时，以“政府整体”作为责任主体的规定也不够明确，将追责主体限定在卫生行政部门，这对大数据多元共治背景下的个人信息损害追责明显保障不足。除了私主体，公权力主体通过数据独裁、滥用等行为，也可能侵犯个人信息权益。而公共卫生相关规范仅明确规定了疾控和医疗机构故意泄露涉及隐私的有关人员信息、资料的责任条款，未明确政府侵害责任；我国《个人信息保护法》第 33 条补充了国家机关处理个人信息的活动适用本法的规定，但不够具体。

其次，就社会组织而言，现有规范缺少对其在数据上报、归集方面的义务要求，导致其参与治理的主动回应度低。公共卫生预警系统个人信息输入主要来自自下而上的“报告”制度，未经报告的重要信息无法进入基础信息库，而信息库来源单一会导致与实际数据的巨大落差、评估滞后等问题[25]。多元信息渠道的扩大能助力大数据治理机制的完善。

最后，就医学专业主体而言，数据处理权责的不确定性使其专业优势未得到有效发挥。一方面，医学机构囿于自身信息系统和存储标准等缺陷，使数据可用性和处理条件参差不齐。现有共享和技术规范也无法满足数据整合应用要求，造成公共卫生数据处理环节薄弱。另一方面，公共卫生相关法律没有明确专业主体参与个人信息治理的具体权责，数据处理规则也无统一标准。如我国《传染病防治法》规定疾控机构有实施传染病预防控制规划及收集、分析、报告传染病监测信息等职责，明确医学院校应为传染病防治提供技术支持，但相关规范较为笼统，未能结合不同信息处理环节作进一步细化。软硬件条件的缺失，使医学专业主体难以主动介入个人信息利用与监督过程。

(三) 个人信息保护行政救济缺失限制权利救济

如前所述，单一私法救济路径在公共卫生数据治理领域存在举证、技术认知和损害认定等困境。借助补强公法的保护性规范来加强实现私法的行为控制，似乎比贸然创造一个轮廓不够清晰的权利更可靠[26]。但是，一方面，公共卫生相关法律规范没有对个人信息权益的事后救济与行政追责加以具体规定，或仅是原则性义务规定。同时，实践中的行政追责通常以行业性准则为依据，对侵害行为仅有弱约束作用，缺乏高层级依据的强监督效果。另一方面，其他有关公共卫生领域个人信息保护的监管立法，散见于《网络安全法》《民法典》《数据安全法》《个人信息保护法》等法规，体系性和针对性不强。其中，《民法典》《个人信息保护法》提出了个人生物识别信息概念，但主要将其涵盖于个人信息概念之中进行统一规范，分别纳入“私密信息”或“敏感个人信息”范畴，没有突出个人医疗信息的强个体关联性下的高脱敏性需求及侵害风险不确定性特点[27]。对于敏感个人信息，《个人信息保护法》专门设节规定了处理规则，包括生物识别、医疗健康和行踪轨迹等类型，但将私密信息仅以知情同意或隐私权保护路径为主进行适用，难以脱离纯粹私法保护路径的举证和救济难题，公共卫生相关法律规范也未能与之适时衔接。

三、公共卫生数据治理中个人信息利用与保护的价值冲突

(一) 公共卫生数据治理的本源价值冲突：个人隐私与公共健康

在公共卫生规制领域，20 世纪雅各布森案曾展现了社会契约论与有限政府理论之间存在的一种紧张关系，而后进一步引发了个人自由权与公共管理权的博弈。随着大数据技术在社会治理制度中的嵌入，现代化公共卫生数据治理领域又增加了数据科学维度与人文维度的价值判断难

题。在大数据治理与公共卫生规制结合的实践中，个人信息保密性与公开性、自主控制性与共享开放性的冲突，在本质上都可归结为个人隐私与公共健康的利益冲突。

数据治理领域以保障个人隐私为基本原则，公共卫生领域以保障公共健康为主要目标，这导致个人隐私和公共健康的利益冲突成为公共卫生数据治理机制中最突出的核心矛盾之一。具体来说，首先，在我国的法学探讨中，个人信息比个人隐私的范围相对更广。美国法学家将隐私权定义为“不受他人侵扰的权利”[28]，可以理解为包括两部分内容：一是独处的权利，二是保有秘密的权利。相比个人信息而言，公众对于隐私在主观上的私密性和保密性需求更突出。尽管不同人群对隐私内容和尺度的理解存在差异，但在公共卫生领域，存在利益冲突的个人信息大多属于具有强敏感性的隐私范畴。其次，公共卫生并不限于单个学科问题，且是理论与实务交叉领域。公共卫生领域事实上可以分割为诸多各自独立的研究分支，包括烟草控制、酒精规制、肥胖问题、儿童健康、流行病防治、疫苗接种等，而保障公共健康是贯穿全部领域的核心宗旨。

从公共卫生规制目标看，某种程度上，尊重个人隐私和促进公共健康是一致的，公共健康取决于公众的信任与合作，如不能全面有效地保护个人权益，就难以鼓励个人参与公共健康项目[29]。然而，一方面，公共卫生治理过程通常包含常态和应急状态相互转变的过渡期，这期间常伴随社会状态性质上的改变。这种状态的转换性会引起规制目标也不断地产生变化，从而使个人隐私、自由利益与公共利益发生矛盾。另一方面，个体健康是“个体的医学”，关注病人个体的状态，而公共健康强调“群体的医学”，更注重个体于群体幸福和安全而言所具有的内在价值[30]。公共卫生通过多方面的规制，拟促进或限制在人群或跨人群展开的保护公共健康的活动[31]。这种服务于人群的公共健康行动，既要保护个体健康，更要防止疾病传播、保护群体免受整体环境危害，在某些情形下，对群体利益的保护不得不放弃或侵害部分个体利益，难以避免存在群体利益需要个人权益的让渡与个人利益需从群体保护中获得的矛盾。

从大数据治理实践角度看，个体隐私与公共健康的矛盾还体现在数据治理机制对个体信息的聚合利用要求与公民对个人信息的脱敏保护需求之间。大数据治理主要通过对多样化数据样本的收集与整合，在海量个人信息聚合基础上，加入专业判断和算法技术进行分析，以求形成一种链式预判结果。但医疗健康信息如虹膜、指纹等，会体现出强个体关联性，即使是匿名化后的身份、行为或行踪信息等，内容上也容易显示个体生活最私密的部分，仍可能具有高度可识别性特征。由此，加强对相关个人信息匿名化、规范化保护，在一定程度上又可能限制大数据聚合的公共利用效能。

个体与群体之间的矛盾与让渡如何通过相应制度加以平衡，理论界有不同观点。西塞罗基于公共本位思想，认为公益优于私益；孟德斯鸠提出，人们要不断地把公共利益置于个人利益之上[32]。康德则更强调个人本位理念；罗尔斯认为每个人都拥有基于正义的不可侵犯性，这种不可侵犯性即使以社会整体利益之名也不能逾越[33]。随着个人权利观念的发展，权益冲突问题也变得越发尖锐，并且是客观存在的。现代国家政府的公共事件管理与规制理念，不应再推崇价值择一，当发生权益冲突时，应通过法律规范来合理权衡利益位阶和明确具体规则，使高位阶权益受到适当倾斜保护，同时限定低位阶权益的干预范围，从而调和种种相互冲突的利益诉求。

(二) 对个人信息私权益的限制：保障公共卫生是价值基础

在我国公共卫生规制领域，从规范层面看，为保障社会公共利益而对个人信息的必要限制行为具有法定依据。《信息安全技术个人信息安全规范》明确了“与公共安全、公共卫生、重大公共利益直接相关”情形下的个人信息收集、使用属于“征得授权同意的例外”，承认了公共卫生治理领域基于公共利益而直接进行个人信息收集、使用的合法性；《个人信息保护法》也将“为应对突发公共卫生事件，或紧急情况下为保

护自然人生命健康和财产安全所必需的情形”排除在个人信息采集必须取得个人同意的规定之外；《传染病防治法》第 12、32、33、68 和 69 条等，分别针对涉疫信息控制、使用行为和追责作了相应规定。

从理论层面看，保障公共卫生作为限制私权益的价值基础也具有正当性。公共卫生通说定义强调群体视角，即“公共卫生是指一般公众或作为整体的社区处于普遍的健康状态，而免于普遍的疾病或死亡”[34]。公共卫生规制以社会正义基础为核心使命，通过关注最弱势群体的需求以实现人类共同福祉的目标[35]。因而，公共卫生体系的核心是增进社会整体福祉，并以保障公众生命安全和普遍的健康为目标。而给人类生命以及其他不可剥夺的法益提供保护，在任何地方都应被视为法秩序的优先任务[36]。尽管对个人信息的保护，发端于个人基本权利，保护的是人的尊严所派生的个人自治、身份利益、平等利益[37]，但当物质性人格权与精神性人格权相冲突时，物质性人格权应处于最高位阶[38]。此外，保护自然人生命权是建立国家的重要目标之一[39]，而保障社会整体利益也是现代国家政府的重要使命之一。社会整体是由个体组成的，公共福祉也是在尽力对个体利益充分保障的基础上得以实现的。保障自然人生命安全与保障公共利益并不完全相悖。公共卫生数据治理理应充分尊重个人信息自主性，避免对私权利的不当损害。但面对突发流行病危机，在全面保障公共安全之前，没有任何个体生命是绝对安全的，过度保护某项个人私权益，反而可能降低对整体公共利益或第三人的保护程度。

总的来说，在公共卫生治理目标整体性视阈下，对患者个体利益的适度限制是为了保障社会集体健康与安全，公共福利是限制个人权益的价值基础。因而，看待个人信息保护与公共安全保障关系的一般逻辑可以依此为原则：个人将自身部分利益分割后交由国家经管并汇总为公共利益，同时公共利益也会对个人权利进行反限制，但应在能够证成出于实现公共利益的切实需要时，才允许对个人权利施加限制[40]。基于整体福祉目标而对脱敏程度高、可识别性低的相关个人信息的系统性获取、利用行为及私权利的适度让步是必要且正当的。但对于涉疫个人敏感信息限制行为的标准，不应止于公共利益价值目标，还应控制在特定情形和限度内。

(三) 限制行为的限度：结合场景化理论厘清边界

科斯曾提出“损害相互性”观点：社会主体总会在自行其是时相互影响，法律无论如何界定权利，都难以实现绝对平衡，只能就主体间的利益冲突，在特定条件下作一个定分[41]。公共卫生领域的多元价值取舍，导致制度安排很难取得实质性平衡。结合数据流动和多元利益的变化，完善个人信息利用与保护限度的划分标准与规则，可以为不同价值取向确定基本界限，在一定程度上增强行为的确定性和稳定性。

海伦·尼森鲍姆的“场景完整理论”强调个人信息保护边界的动态性特征，构建了适用处理数据流(data streams)的模型，有助于以更灵活的思维理解特定细分场景下的行为边界。该理论认为隐私保护问题与不同场景相关联，即对于同类型信息的保护要求，在不同情形下也不完全一致。对于医疗健康、教育、宗教等情境下的隐私数据，人们最关心的并不是如何简单地限制信息的流动，而是确保它在不同场景中能够适当地自由流动[42]。依据场景理论，数据处理参与者对个人数据的存储、监控和跟踪行为是被允许的，但不是绝对自由的。只要在不被禁止的条件下，该行为满足允许干预的限定要求，且是服务于场景的特定目标，在合理规范区间内就应允许信息自由流动。保障公共健康福祉目的为个人信息处理行为提供了正当性基础，但要进一步界定干预行为的具体限度，场景理论的应用为我们开辟了新的思路。

首先，解构公共卫生数据治理场景类型，细化不同场景下差异化规范内容。公共卫生规制所具有的阶段性、不确定性与预防性特点，表明其也强调对区分场景类型的规范化适用方式和敏感个人信息的动态化保护形式的需求。例如，在疫情状态和常规状态、不同风险等级、烟酒控制

或疫苗接种等分支领域、数据公开与共享等不同场景下，个人信息保护力度需求存在区别。同时，在相同场景下，个人信息利用过程还包含采集、披露、加工及后疫情时期数据再利用或被遗忘等不同阶段，需结合不同环节的特殊性，完善相关行为的规范内容。

其次，应结合场景理论，通过动态化思维与规范化方式实施对公共卫生领域大数据的治理。强调动态化思维并非否定确定性，而是要注重不同场景的变化与不同治理主体的优势特点，加强对多元主体的回应互动性与风险应对的调整灵活性的考量。一是依据场景变化，基于不同信息处理主体定位与功能的区别，设定联动化、差异化的权责配置结构。场景理论是在尊重关键信息处理者于不同场景扮演特定角色的前提下，强调数据的安全性和机密性，而关键参与者也有责任和义务保障数据的安全流动、处理和利用[43]。例如，为保障舆论监督，媒体在合理范围内享有收集信息的自由，但没有要求个人必须提供信息的权利；医疗机构有属于公共范畴的职责性质，在特定范围内承担个人信息妥善保护的义务，而在紧急场景下，也应配合行政主体及时上报必要信息。二是在不同场景中，在满足行为合规的前提下，应允许相关信息和行为性质的适当转化。如身份、病情、活动轨迹等信息，于个人而言属于隐私范围，而在疫情场景下，出于公共安全保护之需要，这类信息有了公共性意义，有必要向公众部分公开，保证公众对风险状况的知情和对风险内容的认知，以进一步推进风险防控工作。

最后，当对个人信息利益的公共性干预缺少救济可行性时，应禁止该个人信息利用和限制行为。在缺少有效救济途径的情形下，公权力介入个人私权利行为与个人维护自身利益能力是不对等的，任何场景下的限制行为都不具有正当性。救济可行性要求对救济方法和救济能力等方面有所保障，既需要明确公民个人是否存在合适的救济工具，如对敏感个人信息的私密保护与开放共享规范如何设定，也需要保障被侵害人有足够的可能性实现救济，如当个人司法维权难以证明风险损害或预防性损害时，应加强行政救济途径或改善风险评估方式，提升救济可行性。

四、协调个人信息利益保护与公共卫生安全的建议

(一) 细化公共卫生领域个人信息的差别化公开与共享规则

公共卫生界普遍倡导按照预防原则来管理风险，面对科学不确定性情形下的行动，仍支持进行具有远见规划的主动干预[44]。不同于对既有损害的规避，面对公共卫生风险的预判性干预，即在无法准确判断限制行为与决策效果是否会造成社会影响以及多大程度上的消极后果时，规制的不确定性使原则性的处理规则难以完全匹配具体个案的适用。个人信息相关处理规则需结合具体场景，提升可操作性，才能被有效落实到实践。

首先，公共卫生领域相关个人信息公开规则的完善。第一，明确不得公开的“绝对敏感个人信息”内容。如此规定可弥补现有规范对于涉及公共利益的隐私信息内涵与公开边界认定模糊的缺漏，可适当结合不同场景的风险程度区分划定禁止范围。第二，完善信息披露阶段的信息主体规范内容，包括信息公开主体和被公开主体的规范内容。《传染病防治法》对相关主体的疾病信息通报义务、未尽通报义务的责任以及故意泄露隐私的责任规定相对全面，但关于信息公开阶段的允许披露和被披露主体的身份与条件限定不足。即便在紧急状态下，也不是所有信息控制主体都有权擅自公开全部相关个人信息。第三，鼓励第三方参与对个人信息是否公开的评估裁量。尤其是对个人医疗信息私密性与公开性的判断，应适当弱化行政机关的独立裁量方式，充分考虑医疗机构与疾控中心的专业建议。第四，依据差异化和动态化要求，由政府相关部门和疾控机构根据公共卫生风险分级，综合考量对具体信息类型进行不同程度的差别化披露。

其次，公共卫生领域相关个人信息共享规范的完善。一是考虑到当前多地政府的数据平台都处于“自成一体”的客观局面，要形成数据全面共享，从国家立法层面一时难以实现，可根据区

域现实差别，先从县、市级以出台、细化地方法规办法的形式，层层推进个人信息开放共享规范的制定，并渐进落实④。二是针对数据开放层面，注重放宽上下级、同级部门间的开放内容，除了继续推进由下往上的数据归集要求，更要同步推动上级对下级、不同部门间的数据开放。但在不同层级和部门间应避免主体间无差别共享，如医疗机构与公安部门之间通常不需要共享个人生物识别信息等。三是在数据共享层面，不仅要促进那些无法面向公众开放的公共部门数据被专业研究机构再利用，也要推进政府向市场主体反向的数据获取。美国的第三方准则构建了市场主体参与疫情监测防控的典型模式，具有可借鉴性。当电信运营商、汽车制造零售商、电商平台、媒体等所控制的信息具有高度公共利用性，并且其数据集合能获得与自然灾害、疫情、恐怖袭击等危及国家安全、社会稳定的紧急状态相关的预测时，应明确相关数据经营者主动向国家机构及时公开信息结果的义务[45]。

(二) 协调并明晰多元治理主体的权责与义务规范

现代民法自治有一定局限，而法定主义调整方式又容易损害自治，在该种不及与不能中，需要多元主体参与治理，采用多种方式实现利益的调整[46]。公共卫生数据治理制度安排也需根据主体优势和定位，通过合理规范权责配置，推进多元化治理方式由独立治理向协同共治转变，推进治理状态由被动适配向主动参与转变。

其一，推进政府主体对个人信息利用规制的权责统一。多种社会力量的加入，给治理实践带来责任不明、治理混乱的问题。政府本身是具有公共目的属性的存在，其统筹主导地位有利于协调信息不对称、缓和市场化治理失灵。强化政府的领导与责任主体地位，并不是限制多元共治，而是促进、协调多元主体更合理地行使权利义务，缓解冲突。在公共卫生法律规范中，首先应确认政府对数据治理工作的领导与监督职权，在此基础上，补充对政府的个人信息处理不当、泄露及监督不到位等行为的责任追究，实现权责统一。同时，设立公共卫生领域专门个人信息保护监督机构。《个人信息保护法》未增设专门机构，有必要在特殊领域单设机构作为补充。该机构除了受理个人追责投诉，还要实时监督常态和非常态下的个人信息处理行为。监督对象不仅针对私主体，也包括各级政府及其部门。

其二，明确社会组织对个人信息归集的义务规定。社会组织参与治理，能为行政决策提供科学参考和技术支撑，并发挥其在重点领域的验证、监督和纠偏作用。我国《突发事件应对法》第 38 条规定了县级以上人民政府及其部门、专业机构应通过多种途径收集突发事件相关信息，但没有明确社会组织进行信息归集、报告的特定义务，使得其参与的主动性与能动性体现不足。为增强信息来源渠道的多样性，有必要完善相关规范。例如，将特殊情形下诸如药店销售特定药品的信息、医疗机构出现特殊病例症状的信息、急救中心的电话呼叫和出车记录、单位缺勤记录等，纳入公共卫生预警系统报告范围，并明确相关主体的义务规定[47]。尽管多样化信息渠道可能给预警系统带来信息质量甄别的挑战，但其仅作为一种补足性方式，能在更大信息库范围内促进消息的验证。

其三，赋予医学专业主体在个人信息披露与处理方面的独立性地位。对于新发疾病的病源、病因、传播方式、突发事件发展趋势及相应防控措施的判断，应从权责规范上，适当突出专业主体在信息处理环节的能动性与权威性，及信息披露阶段的独立性。专业主体的介入有助于协调公共卫生规制与决策方面法治化、行政化与科学化的关系[48]。医学院校、科研机构、疾控机构等在与传染病防治直接相关的研究方面，依法独立行使数据处理职能。紧急情况下，允许其基于了解的事实向公众披露必要的风险提示信息，如疑似病例特征、防护信息引导等。但当专业主体存在误判或错误披露等行为时，也应承担相应责任。同时，明确疾控机构的监督权，允许其与专门监督机构对公共卫生个人信息处理行为进行检阅、监督和评估，作出正当性与合理性判断。赋予专业主体一定的独立地位，行为不受行政机关、其他社会团体和个人的干涉，这对抢占危机应对时机有重要意义，也能防止和监督政府权力滥用或

不作为。

(三) 完善公共卫生领域个人信息权益行政救济路径

第一，探索个人信息处理事后评估机制。针对突发性公共卫生事件，规范事后评估机制，加强行政追责，有利于保障私权利。设置事后评估制度的主要目的并不在于对相关主体重新追溯责任，而是回应公共卫生预防要求，及时调整和弥补不确定性风险损害。一是建议制定公共卫生领域个人信息处理安全评估细则。细则应贯穿于个人信息归集、开放共享、利用与决策各个阶段，包括算法评估和程序评估等，如传染病申报流程、传染病报告制度。二是除了公共卫生领域个人信息保护专门监督机构，还应组织疾控机构、社会组织、媒体等主体共同参与外部咨询会议进行评估。三是设立评估反馈机制，要求相关责任主体对评估结论作出必要回应和制定弥补方案。

第二，适当认可公共卫生数据治理领域个人信息的风险性损害。从立法趋势看，《个人信息保护法》已将风险评估作为信息处理者的重要义务，但笔者认为不应止于评估研究。风险性损害的认定是因应风险社会的现实需要，但从风险社会概念中抽象意义的风险到具体法律责任构成要件意义上的风险的转化，还需深入研究[49]。在公共卫生领域个人信息侵害具体认定中，建议进一步延伸与确立“风险”的概念，认可针对个人信息的风险性损害，并细化风险性损害评估要求，以弥补相关损害的认定困境，使个人信息权利救济理念从消除既有损害向预防风险损害适当转变。同时，针对难以评估的个人信息“建构性损害”，在过错推定原则基础上，进一步规定由公共卫生当局承担具体论证责任，并从以下方面作出进阶式系统评估和论证：一是规制理由，即对风险具体情况及其严重程度进行必要阐述，并论证规制行为是否正当合理；二是干预方式的有效性与手段的匹配性，应阐述是否具有其他选择性更优的措施、是否采取了最小限制手段、是否尽力达到使个人利益损害最小化；三是评估公共利益与个人负担的比例，是否在合理范围内；四是针对相关个人信息风险性损害的评估意见，判断案例是否能扩展认定为风险性损害，并阐明考量理由。

第三，完善公共卫生领域场景化敏感个人信息处理与安全保障规则。一是区分在公共卫生常态化数据治理和紧急状态数据治理中，对于敏感个人信息的加密和脱敏处理要求，常态化治理更注重数据存储加密安全，紧急状态下更注重数据流转、共享过程中的脱敏需求，包括对数据共享中二次处理行为的脱敏要求[50]。二是加强规范疫情突发场景下，多元主体在采集、处理个人信息过程中的匿名化要求。在发展匿名化技术的基础上，细化信息控制者及参与治理者的特殊义务与责任规范。三是在突发性公共卫生事件结束后，确认个人信息权利人有权向仍然保有此类信息的监测主体申请删除，即个人信息权利人通过行使“被遗忘权”，请求信息控制者将不具备存在必要性的个人信息予以删除。

五、结语

公共卫生数据治理制度帮助预防已知疾病的流行、提防未知危险的发生或抑制危险扩散，通过机制有效运作能抢得应对危机的先机。治理实践中，为赢得更多的社会公共利益之保全和存续，信息治理主体可能对个人信息私权益有一定程度的限制，但不是无约束地对全部私权益都可以“公共利益”之名进行限制和剥夺，而需要遵守一定的规则。在公共卫生领域，法律应平衡个人信息的利用和保护行为之间的关系，探求个人信息保护与公共卫生保障的价值平衡点。借助场景理论，事实上是将私人和公共领域的差异点放在了同一视野中进行思考，以求妥当地安排信息处理规则和多元主体的权责配置等。公共卫生数据治理制度的完善，重点并不在于明晰两个领域价值边界的具体标准，而是以融合的视野去寻求不同场景下的差异化规范处理方式，以最大限度地保护个人隐私、保障公众健康，并实现信息价值最大化、制度安排最优化。

注释：

① 例如，通过开发应用生物识别技术，将个人基因、指纹、虹膜、面部轮廓等生物特征扫描存储到电子设备以加强身份识别等途径，对于风险的可预测性和认知度将产生质的飞跃，提升风险治理效率。

② 包括《突发事件应对法》《突发公共卫生事件应急条例》《传染病防治法》《基本医疗卫生与健康促进法》《突发公共卫生事件与传染病疫情监测信息报告管理办法》等公共卫生领域相关法律规范。

③ 以 2019 年长沙市数据资源管理局信息化项目调研报告的数据为例，在对市级 53 家单位调研后发现，使用自建系统的单位有 12 家，占比 23%；既使用垂直系统又使用自建系统的单位有 31 家，占比 58%；仅使用垂直系统的单位为 4 家，占比 8%；未使用系统的单位为 6 家，占比 11%。除了共享意识和规范的不足，各自数据平台和系统本身客观上的分割化，也进一步限制了相关数据实现跨主体共享。

④ 目前医疗健康数据共享立法实践先行一步的整体现状，也符合这一进路，多地地方政府已制定相关细则，如《济南市健康医疗大数据应用发展行动方案(2017—2020 年)》《福州市健康医疗大数据开放开发实施细则》等。

参考文献：

[1] 齐爱民. 拯救信息社会中的人格：个人信息保护法总论[M]. 北京：北京大学出版社, 2009: 77.

[2] 梅夏英. 数据的法律属性及其民法定位[J]. 中国社会科学, 2016(9): 164−183, 209.

[3] 化柏林, 郑彦宁. 情报转化理论(上)——从数据到信息的转化[J]. 情报理论与实践, 2012(3): 1−4.

[4] 高富平, 张英, 汤奇峰. 数据保护、利用与安全——大数据产业的制度需求和供给[M]. 北京：法律出版社, 2020: 42−43.

[5] SHU Weiting, CARIN L, DZAU V, et al. Digital technology and COVID-19[J]. Nature Medicine, 2020, 26: 459−461.

[6] 苏今. 后疫情时代个人涉疫信息的控制特点及其路径修正——以隐私场景理论为视角[J]. 情报杂志, 2021(9): 124−132, 123.

[7] 高富平. 个人信息保护：从个人控制到社会控制[J]. 法学研究, 2018(3): 84−101.

[8] FOX D M. From TB to AIDS: value conflicts in reporting disease[J]. The Hastings Center Report, 1986, 16(6): 11−16.

[9] 许可. 重大公共卫生事件的数据治理[J]. 暨南学报(哲学社会科学版), 2021(1): 80−91.

[10] 苏成慧. 论可交易数据的限定[J]. 现代法学, 2020(5): 136−149.

[11] 陈奕青, 张富利. 大数据环境下的国家治理与风险应对[J]. 广西社会科学, 2021(3): 16−25.

[12] JOHN Coggon. What makes health public? A critical evaluation of moral, legal, and political claims in public health[M]. Cambridge: Cambridge University Press, 2012: 7−9.

[13] 徐家良. 疫情防控中社会组织的优势与作用——以北京市社会组织为例[J]. 人民论坛, 2020(23): 28−31.

[14] 王建学. 论突发公共卫生事件预警中的央地权限配置[J]. 当代法学, 2020(3): 54−63.

[15] 张民安. 美国当代隐私权研究：美国隐私权的界定、类型、基础以及分析方法[M]. 广州：中山大学出版社, 2013: 212−213.

[16] 郭春镇, 马磊. 大数据时代个人信息问题的回应型治理[J]. 法制与社会发展, 2020(2): 180−196.

[17] 沈岿. 数据治理与软法[J]. 财经法学, 2020(1): 3−12.

[18] 史卫民.大数据时代个人信息保护的现实困境与路径选择[J]. 情报杂志, 2013(12): 155−159, 154.

[19] 冯果, 薛亦飒. 从“权利规范模式”走向“行为控制模式”的数据信托——数据主体权利保护机制构建的另一种思路[J]. 法学评论, 2020(3): 70−82.

[20] 谢鸿飞. 个人信息泄露侵权责任构成中的“损害”——兼论风险社会中损害的观念化[J]. 国家检察官学院学报, 2021(5): 21−37.

[21] 金自宁. 风险行政法研究的前提问题[J]. 华东政法大学学报, 2014(1): 4−12.

[22] 吴伟光. 大数据技术下个人数据信息私权保护论批判[J]. 政治与法律, 2016(7): 116−132.

[23] 李卫华. 民法典时代政府信息公开中个人私密信息保护研究[J]. 政治与法律, 2021(10): 14−24.

[24] 俞可平. 治理与善治[M]. 北京：社会科学文献出版社, 2000: 9−15.

[25] 金自宁. 风险视角下的突发公共卫生事件预警制度[J]. 当代法学, 2020(3): 64−74.

[26] 冯德淦. 数据的二元划分与体系保护[J]. 中南大学学报(社会科学版), 2020(5): 70−81.

[27] 于洋. 论个人生物识别信息应用风险的监管构造[J].行政法学研究, 2021(6): 101−114.

[28] WARREN, BRANDIES. Right to privacy[J]. Harvard Review, 1890(4): 193.

[29] 李燕. 限制与保护：公共健康领域的个人隐私权[J]. 政法论丛, 2017(2): 76−83.

[30] F.D.沃林斯基. 健康社会学[M]. 孙牧虹, 等译. 北京：社会科学文献出版社, 1999: 9.

[31] 约翰·科根, 基思·赛雷特等. 公共卫生法：伦理、治理与规制[M]. 宋华琳, 李芹, 等译. 江苏：译林出版社, 2021: 7−35.

[32] 孟德斯鸠. 论法的精神[M]. 张雁深, 译. 北京：商务

印书馆, 1982: 34.
[33] 罗尔斯. 正义论[M]. 何怀宏, 等译. 北京: 中国社会科学出版社, 1988: 3−4.
[34] 劳伦斯·高斯汀, 林赛·威利. 公共卫生法: 权力、责任、限制[M]. 苏玉菊, 刘碧波, 等译. 北京: 北京大学出版社, 2020: 12−16.
[35] GOSTIN L O, POWERS M. What dose justice require for the public's health? Public health ethics and policy imperatives of social justice[J]. Health Affairs, 2006(25): 1053−1060.
[36] 卡尔·拉伦茨. 法学方法论(第 6 版)[M]. 黄家镇, 译. 北京: 商务印书馆, 2020: 237.
[37] 高富平. 论个人信息保护的目的——以个人信息保护法益区分为核心[J]. 法商研究, 2019(1): 93−104.
[38] 王利明. 论民事权益位阶: 以《民法典》为中心[J]. 中国法学, 2022(1): 32−54.
[39] 霍布斯. 利维坦[M]. 黎思复, 黎廷弼, 译. 北京: 商务印书馆, 1985 : 序言.
[40] 郭明瑞. 权利冲突的研究现状、基本类型与处理原则[J]. 法学论坛, 2006(1): 5−10.
[41] COASE R H. The problem of social cost[J]. The Journal of Law and Economics, 1960(3):19−28.
[42] HELEN NISSENBAUM. Privacy in context: Technology, policy and the integrity of social life[M]. Stanford: Stanford University Press, 2009: 3−12.
[43] BECKER M. Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy[J]. Ethics and Information Technology, 2019, 21(4): 307−317.
[44] American Public Health Association. The Precautionary Principle and Children's Health[J]. American Journal of Public Health, 2001, 91: 495−96.
[45] 龙卫球. 再论企业数据保护的财产权化路径[J]. 东方法学, 2018(3): 50−63.
[46] 许中缘. 论《民法典》的功能主义释意模式[J]. 中国法学, 2021(6): 183−200.
[47] CHRETIEN J P, BURKOM H S, et al. Syndromic surveillance: Adapting innovations to developing settings[J]. PLoS Medicine, 2008, 5(3): e72.
[48] 陈云良, 陈煜鹏. 论传染病防治决策的法治化和科学化[J]. 比较法研究, 2020(2): 25−39.
[49] 田野. 风险作为损害: 大数据时代侵权“损害”概念的革新[J]. 政治与法律, 2021(10): 25−39.
[50] 金松, 张立彬. 突发公共卫生事件下的个人信息保护研究——以新型冠状病毒肺炎疫情为背景[J]. 情报理论与实践, 2020(6): 16−22.

Utilization and protection of personal information in big data governance in the field of public health

XU Zhongyuan, HE Shucen

(School of Law, Central South University, Changsha 410006, China)

Abstract: The use of personal information is a core element of big data governance in public health. In China's public health data governance, there are practical problems such as balance between the privacy of personal information and conflict of public value, the dilemma of information integration among multiple governance subjects, and relief impediment of private law remedies for constructive damage to personal information interests. The lag of relevant laws and regulations in the field of public health in big data governance and personal information protection rules is the superficial reason that hinders the efficiency of information utilization and weakens the protection of rights and interests. The value contradiction between personal privacy protection and public health protection is the theoretical root cause. To restrict the private interests of personal information, we should take guaranteeing public health security as the legal basis and value basis, abide by the differentiated and dynamic compliance processing rules which are based on contextual deconstruction as well as the limit requirements for remedies. And we should improve relevant legal norms, including specifying the differentiated disclosure of personal information, sharing of personal information, clarifying the allocation of powers and responsibilities of multiple subjects, and strengthening administrative supervision and remedies for personal information rights and interests.

Key Words: public health; big data governance; sensitive personal information; conflict of interest; contextual integrity theory

[编辑: 苏慧]