个人信息在智慧治理中的风险与保护

——以《民法典》个人信息保护为中心

方志伟 王建文[1]

【摘 要】：伴随着大数据、人工智能等技术在社会治理领域的长足发展，政府利用个人信息实现智慧治理得以可能。但行政机关在收集、加工、使用、共享等处理个人信息过程中存在诸多风险，且现行法律体系对规制政府利用个人信息的制度供给严重不足。《民法典》作为私权领域的基础性法律，明确了公民个人信息受法律保护，具有规范、平衡和指引政府处理个人信息的重要意义。未来需要在《民法典》的框架下，通过制定个人信息在公共领域合理使用规则，明确行政机关的责任形态，完善对个人信息主体的损害赔偿制度，促使政府在智慧治理中合理利用个人信息。

【关键词】：民法典 智慧治理 个人信息智能处理风险 个人信息保护

【中图分类号】D920**【文献标识码】**A**【文章编号】**1004－518X（2021）05－0179-13

近年来，个人信息的公共价值已在公共管理中得到广泛利用。在大数据、人工智能等技术的加持下，政府部门可以低成本、高效率地收集和处理更多个人信息，实现科学、理性的决策[1](P38-59)，传统政府治理模式逐渐转向数据治理并最终实现“智慧治理”。政府利用人工智能技术革新其履职模式，但个人信息利用的边界及发生个人信息侵权后的救济规则等并无直接的法律法规予以明确。

效力位阶较高的《网络安全法》虽然对个人信息的范围和使用方式有所提及，但其所规范的主体是可能侵害个人信息的“网络服务提供者、运营者”“其他企业事业单位”等，政府部门在《网络安全法》中的定位是纯粹的监管者和个人信息保护者，而非个人信息的获取者和使用者。[2](P2-14)党的十九届四中全会明确提出，“要建立健全运用互联网、大数据、人工智能等技术手段进行行政管理的制度规则”[1]，个人信息的规范利用必然是其应有之义。

令人欣喜的是，《中华人民共和国民法典》（以下简称《民法典》）就个人信息的内涵、使用方式、生命周期等作了详细规定，个人信息所蕴含的价值及其权利（权益）属性获得私法之确认。因此，当下的紧迫任务是如何在《民法典》的框架下探究个人信息在智慧治理过程中的利用方式与限度，完善公共领域个人信息保护的法律体系，实现个人信息安全与政府治理高效运行之间的平衡。

一、个人信息在智慧治理中的风险

政府作为个人信息最大的拥有者和使用者，存储了海量的个人信息[3](P103-107)，智慧治理即是通过收集、整合大量个人信息形成结构化数据，利用深度学习、数据挖掘等人工智能技术构建算法模型，实现智能化决策、优化公共服务。《民法典》对个人信

[1]**作者简介**：方志伟，河海大学马克思主义学院博士生；（江苏南京 211100）南京航空航天大学网络与人工智能法治研究院研究人员。（江苏南京 211521）
王建文，南京大学法学院教授、博士生导师。（江苏南京 210093）
基金项目：国家社会科学基金重大项目“优化市场化法治化国际化便利化营商环境研究”（21ZDA052）;江苏省研究生科研与实践创新计划中央高校基本科研业务费专项资金资助(2016B48014)

息处理作了较为详尽的规定，其将个人信息的处理分为收集、存储、使用、加工、传输、提供、公开等。[2]依据《民法典》关于个人信息处理的分类，结合智慧治理过程中对个人信息利用的实践现状，笔者认为个人信息在被政府收集利用过程中可能存在如下风险。

（一）信息收集：过度或违规收集个人信息

目前，我国各地关于政府对个人信息收集的内容、采集方式仍在探索之中。在《民法典》个人信息保护的框架下，政府收集个人信息过程中可能给个人造成以下风险。其一，过度收集个人信息。《民法典》颁布前，行政机关对个人信息收集并无细致规定，智慧政务平台、政务 APP 超范围收集个人信息时有发生。本文写作过程中，笔者登录某公安局智慧警务平台，即被要求“允许使用你的地理位置”，这已明显超出必要的收集限度。

此外，不同政府的智慧政务平台办理相同事务收集的信息范围却不尽一致，如公积金查询服务，浙江省比河北省的智慧政务平台多出人脸识别的要求，相较之下，浙江省智慧政务平台难免存在过度收集个人信息之嫌。其二，违规收集个人信息。政府智能收集个人信息行为可能存在有意或无意的违规，以广受称赞的“天网工程”[3]为例，该工程通过星罗棋布的视频监控设备，对特定区域进行实时监控和记录，为我国公共安全构筑起重要防线。诚然，愈发密集的“天眼”确能有效识别犯罪嫌疑人，维护社会稳定，但也近乎完整地覆盖监控范围内其他公民的行为和状态。在未经广泛的公众参与、未出台配套细则及救济机制的情况下，贸然展开大范围的视频监控联网建设，其对公民个人信息甚至隐私可能产生的影响让人不寒而栗。[4](P31-46)

（二）信息加工：违法分类标注个人信息或过度关联挖掘

信息加工是对原始信息进行去伪存真、由此及彼的二次信息活动过程。政府机关基于公共服务、社会管理的职能，积累了大量的个人信息，但这些原始信息无法为计算机所理解和应用。直言之，只有经适当加工的个人信息才能用于智慧治理中的预测、风险评估或提供决策依据。个人信息的加工主要利用数据挖掘技术对个人信息数据进行清洗、分类、标注等转化为结构化数据，再经聚类、回归等算法进一步挖掘形成更具价值的个人信息数据库。

人工智能时代，政府对个人信息的加工流程愈发复杂化、自动化，导致个人信息安全风险也愈发突出且隐蔽，从信息加工的过程来看，这些风险主要表现在如下方面。

其一，个人信息的违法标注。个人信息加工需人工或机器进行分类标注，但实践中为实现某些行政目的，行政机关甚至采用违法的分类标注方式。如 2011 年深圳举行第 26 届世界大学生运动会期间，深圳警方利用大数据技术对 8 万名“高危人员”予以标注并将其清出深圳，其分类标签毫无法律依据，如：“没有正当职业，生活规律异常或经济来源可疑的人员”，“有犯罪前科，且无正当职业及合法经济来源”，等等。[5]违法标注的个人信息因缺乏代表性并存在数据偏见，据此训练的人工智能算法必将产生算法歧视和偏见[6](P82-90)，进一步放大智慧治理的技术风险。

此外，由于个人信息载体的多样性（如文字、图片、视频等）及技术的局限性，导致对个人信息的错误标注时有发生。如泉州市某公安局个人信息系统因新老身份证号码更替原因，错误地将某犯罪分子的行为标注在其他人名下。[4]其二，个人信息过度关联聚类。数据挖掘的一项重要功能即在于发现不同信息之间的关联性，但人工智能算法通过回归、聚类等方法挖掘出不同个人信息之间的关联关系是一种概率体现，而非实际的因果关系。个人信息在智慧治理中最重要的价值体现在于将大量的不同类型的个人信息关联、整合在一起用于预测、评估甚至自动化决策。政府通过整合关联个人信息能有效地优化政务流程，提升服务效率，但实践中也存在某些以关联性取代因果判断的行为，并据此对个人信息主体采取不当限制。

（三）信息使用：滥用个人信息

政府对个人信息的使用范围和使用方法在人工智能时代愈发广泛和多样，其在社会风险治理、政策制定等领域都发挥了重要作用。在享受大数据和人工智能带来的便利的同时，我们还应注意到，行政机关作为个人信息使用者时，监督机构的缺位极易引发个人信息滥用的风险。例如，2014 年江苏睢宁县推出大众信用体系评级系统，是基于个人信息利用的一种探索，旨在提供一种现代市场服务，营造“一处守信，处处受益；一处失信，处处制约”的社会氛围。[5]但该信用体系存在将个人行为责任扩大化之可能，当地居民若干“失信”行为将限制其申请国家救济。[7]此即利用有关个人信息限制公民的基本权利，是一种典型的个人信息滥用。再如，有些地方政府利用职务之便收集“上访户”的活动轨迹信息，从而实施“截访”等行为，这无疑是对个人信息的一种滥用，甚至是违法使用。

（四）信息共享：显名共享个人信息

信息开放共享是我国一项重大战略方针，是大数据时代基于政府信息公开制度的时代发展。同时，行政机关基于不同的社会治理目的积累了大量的个人信息并内化为各类政务数据。为实现个人信息公共价值最大化，促进数字经济发展和社会治理变革，2015 年出台的《促进大数据发展行动纲要》中明确各类政务信息“以共享为原则，不共享为例外”。为此，全国各级政府积极推进信息共享开放并设立政务数据开放平台。我们可将政务信息共享开放简单理解为政务信息提供的过程，可以是不同政府部门的内部传输流动，也可以是政府机关共享给其他第三方主体，如企业、自然人等。

然而，囿于缺乏合理适度的开放共享法律法规和政策体系，行政机关对包含个人信息的政务信息共享尺度把握不准，导致个人信息甚至隐私信息的泄漏。如江西省黎川县共享的《关于黎川县 2017 年度建档立卡贫困户名单的公示》文件中，披露了该县近万名贫困户的姓名、身份证号码等个人信息甚至还包含健康状况等私密信息。[6]此外，如果各种不同类型的个人信息不经去标识化共享，即可通过整合分析，再现某特定个体的生活全景，将各自然人变成透明人，形成监控社会。[4](P103-107)

大数据、人工智能技术在政务活动中的广泛应用，使公共领域利用个人信息的方式、空间发生巨变，并在不同的处理环节衍生出不同的安全风险。此外，新型技术的加入，还将加剧传统模式下政府机关侵害个人信息的风险。如政府信息公开过程中的个人隐私侵犯，因网络传播的即时性和广泛性将无限放大个人隐私权益侵害的影响面。人工智能时代对于个人信息的保护早已不再着眼于限制个人信息的收集和利用，防止个人信息滥用及造成财产和隐私等损害方是重中之重。[8](P53-61)因此，个人信息在公共领域的利用，尤其是智慧治理场景中的利用亟待出台相关制度予以规制。

二、个人信息在智慧治理中法律保护的现状与不足

随着信息技术的发展，人们对个人信息利用的多样化，导致对个人信息的保护也显得愈发迫切。早在 21 世纪初个人信息保护就已引起学界的广泛关注，多位学者就个人信息保护相继提出了相关立法建议稿。[7]时至今日，个人信息保护法仍在制定当中。实践中人们时常通过援引政府信息公开相关条款对政府不当利用个人信息予以规制。[9](P51-55)但人工智能时代，政府对个人信息的利用早已超越信息公开的使用目的。因此，仔细梳理现有的政府利用、保护个人信息的法律法规，发现其中的不足之处就显得尤为必要。

（一）政府处理个人信息的制度依据

如前所述，政府作为个人信息的最大存储者和使用者，相应地，其对个人信息的侵权风险也最大，对个人信息保护的责任也最大。通过检索现有法律法规体系，目前有 50 部法律、60 多部行政法规及数百部部门规章对个人信息的利用和保护作出或多或少的规定[8]，但其中政府的角色多为监督者和管理者。具体至公共领域，个人信息的利用和保护则鲜有涉及，而更高级的利用——基于数据挖掘的个人信息聚合利用——规制则近乎“真空”状态。

在公共领域，政府处理个人信息的相关法律法规较为稀少，个人信息利用的相关制度十分零散，个人信息的使用范围、使

用方式、责任主体、责任内容等都不甚明确。笔者通过梳理在全国范围内统一施行的法律、法规、规章，发现政府处理个人信息的制度依据[10](P134-140)如表 1 所示。

表 1 公共领域政府处理个人信息的制度依据

规定内容		法律、法规、规章
个人信息处理的范围		《民法典》第 1034 条，《网络安全法》第 76 条，《居民身份证法》第 3 条，《护照法》第 7 条，《人口普查条例》第 12 条
个人信息主体权利	知情权	《民法典》第 1035 条，《网络安全法》第 41 条，其他
	决定权	《民法典》第 1037 条，《网络安全法》第 43 条，《政府信息公开条例》第 23、24、25 条，《婚姻登记档案管理办法》第 15 条
行政主体义务	使用限制	《民法典》第 999 条，《统计法》第 25 条，《统计法实施条例》第 30 条，《人口普查条例》第 33 条
	妥善保管	《民法典》第 1038 条，《网络安全法》第 42 条，《国家健康医疗大数据标准、安全和服务管理办法》第 16 条，《统计法》第 6 条，《人口普查条例》第 26、32 条，《婚姻登记档案管理办法》第 13 条
	保密义务	《民法典》第 1039 条，《统计法》第 9、25 条，《食品药品监督管理统计管理办法》第 8 条，《统计执法监督检查办法》第 22 条，《全国经济普查条例》第 32 条，《人口普查条例》第 4、33 条，《政府信息公开条例》第 15 条
侵权责任	刑事责任	《刑法修正案（九）》第 17 条
	行政责任	《居民身份证法》第 19 条，《护照法》第 20 条，《统计法》第 37、38、39 条，《行政许可法》第 5 条，《统计执法监督检查办法》第 46 条，《食品药品监督管理统计管理办法》第 8、25 条，《人口普查条例》第 34、35 条
	免责事由	《民法典》第 1036 条

2013 年以前，立法机关对个人信息内涵的理解较为局限，集中在传统的姓名、住址、电话号码等，政府机关对个人信息的处理也主要集中在公共管理过程中的行政登记、公开等。随着信息技术的发展，个人信息的公共价值愈发凸显，其内容范围逐渐得到扩展，处理方式也逐渐变得复杂，因而《网络安全法》《民法典》等对个人信息的内涵和处理过程作了较为明确的规定。个人信息主体权益内容在立法上仍处于探索阶段，目前仍以人身性权利为主要规制逻辑，其中知情权[9]是个人信息处理过程中信息主体最基本的权利，在多部法律法规中均有体现。此外，《民法典》首次完整地提出个人信息主体的决定权，即赋予其查询、

复制、更正、删除的权利。

（二）对政府利用个人信息法律规制存在的不足

随着《民法典》的出台，我国个人信息的法律保护在刑事、民事、行政等诸多部门法中得到体现，并逐渐体系化。但纵观现行法律法规，其仍存在明显短板，即强调信息主体对个人信息的控制，而对信息处理的具体过程关注不足，尤其是政府部门对个人信息的使用规范问题，立法上更是处于基本空白的状态。具体而言，在《民法典》框架下，现行法律法规对政府处理个人信息实现智慧治理的规制存在如下不足。

1.重视个人信息大数据赋能政府治理，忽视个人信息智能化处理的风险。

基于数据的决策模式正逐渐推动政府治理向人工智能精准治理的范式转变，公民个人信息等数据成为政府治理社会、提供公共服务的重要资源。为此，我国出台了多部法规、规章及政策文件等鼓励或引导利用大数据、人工智能等技术推动智慧治理平台建设。例如，2018 年国家卫健委为促进“互联网+医疗健康”发展，发挥健康医疗大数据作用，制定了《国家健康医疗大数据标准、安全和服务管理办法》，国内多地政府也纷纷出台了类似涵盖个人信息的大数据管理办法，如《赤壁市政务大数据管理办法》《四川省健康医疗大数据应用管理办法（试行）》等。

涵盖个人信息的大数据正加速改变政府治理模式，而对个人信息处理的过程和方式也正由人工处理演变为计算机处理并逐渐向智能化处理过渡。但人工智能对个人信息的智能化处理较之传统的信息处理方式，将带来诸多新的潜在威胁。例如，数据挖掘技术使个人信息利用的广度和深度被无限放大，这意味着政府机关等个人信息处理者可以利用深度学习等算法推断、预测、披露之前个人信息主体并未同意提供的个人信息甚至是个人隐私。有实验证明，利用种族、宗教信仰、父母婚姻状况等个人信息，人们便可极为准确地推测其性取向。[11]

实践中，美国曾有选民通过系统分析个人是否全国步枪协会成员和计划生育支持者，预测用户的选举倾向。[12](P108-117)政府智能化处理个人信息，将对个人信息（隐私）带来极大的安全隐患。同时，政府作为个人信息的最大持有者，导致这种隐忧还将进一步加深。如上所述，现行法律体系对个人信息、大数据等立法取向倾向于促进和利用，而对个人信息利用的法律规范则极少提及，且十分零散地分布在不同的法律、法规之中，导致难以应对人工智能技术对个人信息处理带来的风险。

2.强调个人信息处理结果保护，忽视处理过程的风险。

梳理现行有关公共部门处理个人信息的法律体系，其主要对个人信息处理的结果予以规制，即强调政府部门应妥善保管（保密）合法公开收集到的个人信息，对行政机关收集、加工、使用、传输等其他个人信息的处理过程规制不足。如《统计法》规定统计机构及工作人员对在统计工作中知悉的个人信息应当予以保密；再如，《政府信息公开条例》中规定：“政府信息中涉及商业机密、个人隐私，公开会对第三方合法权益造成损害的，行政机关不得公开。”[10]在以往的行政活动中，个人信息的收集多是基于行政记录统计的结果，加上行政机关对个人信息处理能力的不足，因而政府部门处理个人信息的法律规制集中于对结果的规制也是顺理成章。

但随着芯片技术发展带来的算力飞速提升，个人信息的价值在大数据、人工智能等技术的加持下被无限放大，已在精准扶贫、公共管理等领域发挥了重要作用。智慧治理情景下，个人信息不仅仅是政府日常行政管理过程中的“副产品”，还将是政府部门重要的决策依据。但另一方面，在依法治国的前提下，智慧治理同时仍须是依法治理，政府部门在利用个人信息优化公共管理、提升公共服务的全部过程须在法治的框架内进行。易言之，智慧治理场景中对个人信息收集利用的全部过程应于法有据，即法律对个人信息的保护不仅局限于对结果的保护，还应对个人信息的收集、加工、使用、共享等过程予以规范。但现行法律体系对此极为欠缺，亟待完善。

3.侧重对责任主体的处罚，忽视信息主体权益救济。

如前所述，现行法主要侧重政府部门对个人信息利用及利用结果的法律保护，具体表现为政府部门及其工作人员对收集的个人信息应妥善保管并保密，如有发生泄漏或不当公开应承担相应责任。遍阅现行法中政府部门泄漏个人信息之责任承担，多表现为对违法行政机关及工作人员以罚款、拘留等处罚，情节严重的甚至还将面临刑事处罚。[11]但个人信息主体作为真正的受害人，其个人信息权益的损害却无从救济。个人信息的权益属性在学界一直存有很大争议，有学者认为个人信息属于民事权益中的人格权，也有学者认为个人信息还具有财产属性。[12]

《民法典》对此予以明确，即公民个人信息权益属于人格权益，而非财产权益。[13](P1-18)因此，根据《国家赔偿法》的有关规定，行政机关对侵犯公民合法权益造成的损害应予以赔偿，而对人格权部分的赔偿范围一般限于对生命健康、人身自由等人格权益及其造成的精神损害。[13]可见，个人信息权益不在《国家赔偿法》的赔偿范围之内，在智慧治理场景下行政机关对个人信息权益造成的损害救济将面临无法可依的困境。

给予个人信息法律保护的讨论由来已久，但在智慧治理具体应用场景中的法律保护却近乎空白。纵览现行个人信息保护的法律体系，从立法取向来看，现行法律多倾向于强调利用个人信息赋能政府治理，实现智慧治理，较少关注政府机关如何规范利用个人信息；从立法内容来看，现行法多倾向于结果保护及相应的行政责任，而较少关注个人信息处理的过程规范和个人信息主体损害之救济。值得庆幸的是，《民法典》的出台为个人信息保护在智慧治理场景下提供了方向性指引。

三、《民法典》对公共部门利用个人信息的价值

现代法治核心在于规范公权，保障私权。一般认为，规范公权是公法的主要任务，而保障私权则由私法来实现。但实际上，私法通过确认和保护私权，并成为依法行政的基本遵循。各级国家机关在履行行政职责、实施行政行为时须明确行政活动的范围与界限，不得侵犯公民享有的合法民事权益，包括人身权利和财产权利。[14]因此，从这个意义上来讲，《民法典》作为私权领域的基础性、综合性法律，明确了公民个人信息受法律保护，具有规范、平衡和指引政府处理与利用个人信息的重要意义。

（一）个人信息权益的私法确认

《民法典》出台前，我国个人信息法律保护以公法保护为基调，即主要通过《网络安全法》为主线，借鉴欧盟与美国的有关立法经验，构建起我国个人信息法律保护的基本框架。[14](P3-23)但以《网络安全法》为框架的公法个人信息保护体系所规范的可能侵害个人信息权益的主体是“网络服务者”“经营者”等，行政机关在其中扮演的是监管者、监督者，而非个人信息处理者。令人欣慰的是，《民法典》通过对个人信息权益的调整对象、权益边界等予以私权确认，填补了这一漏洞。

《民法典》将自然人的个人信息有关权益法定化，并为个人信息的保护提供了基本原则和规则。具体至个人信息智慧治理应用场景下，首先，《民法典》将个人信息处理者的范围扩大至“任何组织和个人”，政府作为个人信息处理者之一也将受到《民法典》的调整；其次，《民法典》明确个人信息的判断标准——可识别性，且可识别性不仅包括身份信息还适用于活动信息，如行踪信息、健康信息等，从而扩展了个人信息的保护范围，这也回应了人工智能时代个人信息保护的新诉求；最后，《民法典》还确定了个人信息处理的基本原则，《民法典》在承接了《网络安全法》第41条的基础上，增加了“不得过度处理”的原则[15]，这对个人信息的处理提出了进一步要求，给予个人信息以全生命周期的保护。

事实上，个人信息保护的最终目的是维护自然人的合法权益，即便公法对个人信息保护的相关规定是出于维护公共利益的目的，其根本目标也无法偏离保护自然人的人身财产权益[15](P26-43)，无论是行政法对个人信息利用的规制还是刑法对侵害个人信息的处罚，其目的都是为了保护个人信息这一民事权益。因此，《民法典》通过赋予自然人个人信息相应的民事权益，可以为公法对任何组织、个人收集、存储、使用、加工、传输、提供、公开个人信息等行为规制，奠定民事权益上的正当性基础和民事

基本法的依据。

（二）平衡个人信息的利用与保护

从个人信息保护的角度来看，无论是行政机关还是商业机构，只要掌握个人信息，均存在滥用或侵犯个人权利之可能。[16](P39-40)因此，有不少观点提出个人信息的保护不仅需要对商业企业予以规制，还需要限制行政机关。[16]但事实上，任何国家或地区对个人信息的保护都不是简单限制使用，还必须平衡多种利益，其中最为核心的莫过于个人信息利用与个人信息保护的平衡。从比较法的视角观察，日本《个人信息保护法》第 1 条就明确指出，“在充分顾及个人信息有用性的同时对个人信息的权利利益加以保护”；我国台湾地区的“个人资料保护法”在开篇即明确指出，立法目的在于“规范个人资料之搜集、处理及利用，以避免人格权受侵害，并促进个人数据之合理利用”。[17]

为有效协调个人信息保护与合理利用，《民法典》通过确认个人信息权益性质及其保护规则的同时，还规定了完善的个人信息使用制度，从而实现个人信息的利用和保护之间的平衡。就个人信息的使用制度观察，《民法典》在“知情同意”的框架下，另辟例外原则，平衡个人信息的利用与保护。其一，维护公共利益，如国家安全、公共卫生等公共利益；其二，保护民事权益，如保护自然人的生命健康、财产安全等重要民事权益；其三，合法公开的个人信息，可在法律范围内自由使用。[18]易言之，《民法典》为实现智慧治理提供了完善的制度环境，政府机关基于公共利益或保护民事权利等目的，可以合理收集、处理、存储、共享、公开相关的个人信息，从而加快推进“互联网+政务服务”的部署。

（三）注重事前预防与事后救济相结合

人工智能时代到来之前，行政机关是个人信息收集的主要主体，收集方式也大多由自然人主动填写提交，行政机关等主体对收集后的个人信息以纸媒或是电子存档，不仅信息收集的效率、范围有限，且受限于羸弱的算力、算法，行政机关对个人信息的利用十分有限，多数个人信息仅具统计意义。对自然人个人信息价值挖掘能力的欠缺使个人信息法律保护多为事后救济，强调行政机关及其工作人员收集、处理自然人个人信息过程中的保密与安全保管责任。

人工智能、大数据、物联网等技术赋予个人信息以空前的价值，但也从不同方面对个人信息的保护提出了挑战。在步入人工智能时代后，个人信息处理者收集、存储和利用海量的个人信息，个人信息权益一旦受到侵害，不仅受害人数量极为庞大，且对受害人的损害结果往往具有不可逆性，这就需要强化个人信息保护的事前预防功能。有鉴于此，《民法典》高度重视对个人信息保护的事前预防与事后救济的结合。一方面，《民法典》对个人信息收集、存储、使用、加工、传输、提供、公开等行为予以规制，从源头控制违法收集、使用等行为，发挥损害预防功能；另一方面，《民法典》在人格权编一般规定与侵权责任编对侵害个人信息的损害结果给出了详尽的事后救济路径，实现个人信息保护的事前预防与事后救济的结合。因此，在《民法典》视域下，政府部门既要在收集处理个人信息的过程中遵守相关法律、法规和技术标准，并采取必要的技术措施确保个人信息安全，还应对其违法行为承担相应的责任。

综上，《民法典》的出台对个人信息保护具有重要意义，其不仅规制一般民事主体处理个人信息，同样还规范指引行政机关合法、合理利用个人信息。习近平总书记强调，各级政府要以保证《民法典》有效实施为重要抓手推进法治政府建设。[17](P4-9)作为国家行政机关在人工智能时代的治理模式，智慧治理应把《民法典》作为其处理个人信息的标尺，秉持以人民为中心的原则，充分认识和尊重民事主体的各项权利。

四、《民法典》视域下智慧治理中个人信息保护路径

《民法典》在我国立法历史中具有里程碑式的意义，确定了一系列具体民事权利，其中，人格权得到系统确认与保护并将个人信息保护独立成章是我国《民法典》的最大亮点。[18](P3-13)一般认为民法调整的是平等主体之间的人身和财产关系，但我国《民

法典》对个人信息保护的相关规定对规范公共领域的个人信息利用也具有重要价值。无论是正在制定的《个人信息保护法》《数据安全法》等法律法规，还是既有个人信息保护法律法规的解释适用，都应充分尊重和保护自然人的个人信息，做好与《民法典》的衔接过渡，实现公共领域的个人信息保护与利用。

相较于商业领域，学界对公共领域个人信息的保护与利用的研究屈指可数，多数研究集中于一般私主体在人工智能时代利用个人信息的规制必要性与制度建构，对政府机关利用个人信息实现智慧治理过程中所扮演角色的探讨凤毛麟角。但国内的研究也意识到政府不能肆意收集和利用个人信息，个人信息法律保护的发展始终伴随着对政府权力的限制。[1](P38-59)在《民法典》的规范指引下，笔者认为，我国公共领域个人信息保护与利用，应从构建合理使用的规则体系与权益救济体系等方面予以完善，推动法律制度的立改废释和公法、私法融合。

（一）制定公共领域“合理使用”规则体系

《民法典》在确认个人信息权益的同时，也高度重视个人信息的利用与保护，通过构建自然人与信息处理者之间的权利义务框架，合理平衡了个人信息与维护公共利益之间的关系。[19]显然，立法机关也注意到对公、私部门利用个人信息的限制应该有所不同。通常公共部门处理个人信息是为了更好地实现国家治理、社会管理和公共服务，《民法典》也赋予其“合理使用”的相关权限，但仅保留了相关原则性规定，且配套制度并不完备。概言之，为确保个人信息在公共领域的合理使用，实现智慧治理，我们在个人信息保护的制度体系中需回应个人信息使用的目的与范围、个人信息使用的具体内容、个人信息的使用方式等。

首先，明确个人信息在公共领域合理使用的范围，即个人信息的使用场域。为充分发挥个人信息的社会治理价值，《民法典》明确指出，“为维护公共利益或者该自然人合法权益”，可以合理实施信息处理行为而不承担民事责任。《民法典》为个人信息的合理使用与实现智慧治理创造了接口，但何为公共利益、何为合理信息处理行为均需进一步细化。笔者认为，正在制定的《个人信息保护法》可借鉴《土地管理法》的立法技术[20]，可就“维护公共利益”做列举性说明，如公共卫生防控、技术侦查等，从而明确个人信息利用的逻辑前提。

其次，明确不同使用场景中个人信息的使用内容。区分不同类型的个人信息以确定利用和保护程度，是各国个人信息法律保护的一般路径，我国法律也不例外。《民法典》将个人信息区分为一般个人信息与私密信息，并将私密信息归入隐私权予以保护，但私密信息如何利用和保护并未有明确答案。此前，张新宝提出，将个人信息区分为个人敏感隐私信息与一般个人信息，并强化对个人敏感信息的保护，对个人敏感信息的处理一般被禁止，而公务机关执行法定职务是例外。[1](P38-59)笔者认为，对政府处理个人信息行为仅此限制不免失之过宽，如何赋权行政机关处理何种类型个人信息，仍需进一步细化。正在制定的《个人信息保护法》可通过列举行政机关在不同使用场景中使用何种类型个人信息，从而明确区分私密信息与一般个人信息。此外，对私密信息的利用应当获得狭义法律的授权；而对个人一般信息的利用，可以允许法规作为授权依据。[2](P2-14)

最后，明确行政机关利用个人信息的方式。行政机关利用个人信息实现智慧治理的方式可总结为三种：一是行政机关利用海量个人信息，整合、建模，用于完善社会治理能力或是辅助其他行政决策；二是利用个人信息主体的各类行为数据描绘其“数据画像”（profiling），进而执行某项行政决策，如行政审批；三是利用个人信息主体的直接识别信息（姓名、身份证号等）或间接识别信息（健康信息、行踪轨迹等），识别特定对象身份，如识别犯罪嫌疑人等。不同的利用方式所带来的个人信息权益风险等级并不一致，对其利用方式的限制也应有所区别。对于第一种利用方式，行政机关在不识别特定信息主体身份的前提下，利用海量个人信息建模分析，评估预测社会安全、配置社会资源等，从而提升社会治理水平。该利用方式下，个人信息权益安全风险表现为信息处理者泄漏或是篡改个人信息。对此，《民法典》明确“信息处理者不得泄露或者篡改其收集、存储的个人信息，但是经过加工无法识别特定个人且不能复原的除外”[21]。对于利用不特定多数人的个人信息优化公共服务的方式，应尽可能地去标识化（匿名化）处理。事实上，政府实现上述功能也确实无须识别特定个体身份。第二种利用方式，即通过描绘自然人的数据画像，提供个性化服务，但实践中行政机关却利用数据画像给予信息主体不当限制与歧视，用关联性替代因果关系。因此，对于该利用方式应审慎应用，谨防为实现某行政目的，滥用用户数据画像。第三种利用方式多基于维护公共安全，政府利

用直接或间接识别信息识别个体身份，但却极易对个人权利产生巨大威胁，行政机关极易利用信息技术将普通个体完全置于监控体系之下。因此利用个人信息识别个体身份应被界定为技术侦查，仅在触犯特定罪名时方可使用。[2](P2-14)综上，行政机关利用个人信息实现智慧治理应结合不同应用场景，明确具体的利用方式，实现《民法典》中关于个人信息的利用与保护的平衡。

（二）明确公共信息处理者“安全保障”与“合理使用”的双重责任

《民法典》在人格权编与侵权责任编对个人信息主体的权利、信息处理者的义务进行了一定界分，但在智慧治理的场域下，个人信息侵权的救济需进一步明确作为信息处理者的政府机关之责任。

在人工智能时代，行政机关在智慧治理场景下的法律责任应分为“技术性”责任与“应用性”责任。一方面，智慧治理的实现有赖于处理海量个人信息的软件和提供算力、载体的硬件系统，但系统漏洞、黑客攻击等不确定因素也“如影随形”，威胁着系统中海量个人信息的安全。此外，即便是目前较为成熟的人工智能技术（如语音识别、图像标注等技术）仍存有小概率错误可能，导致个人信息混淆、丢失等风险。由此，行政机关作为信息处理者“应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失”[22]，如独立硬盘冗余阵列（RAID10）、CPU 冗余设计、双机热备份等。只有明确了政府的数据安全保障义务与责任，才可以有效保障数据安全[19](P3-12)，此即行政机关及其工作人员在安全保障方面的技术性责任。另一方面，行政机关利用人工智能技术处理个人信息在实现智慧治理的同时，还可能有意或无意超目的或超范围地利用个人信息实施如前所述的“截访”等非法行为。人工智能技术本身并无善恶之分，也不具备责任能力。但行政机关以“非法目的”处理或使用个人信息必无“合理使用”之可能。[20](P85-92) 易言之，行政机关应在合理使用的规制体系内利用个人信息，对于不合理使用个人信息的行为对信息主体造成的歧视或不当限制，应承担相应的应用性责任。

当前，我国《民法典》对信息处理者的技术性责任与应用性责任均作出了原则性规定，并强调了有关行政机关及其工作人员对于履职过程中获取的个人信息和隐私的保密义务。[23]《民法典》作为典型的私法，对行政机关及其工作人员的规制稍显不足，且相对宽泛。因此，正在制定的《个人信息保护法》等个人信息保护立法，应在《民法典》的框架下，结合智慧治理的具体使用场景予以细化，明确行政机关及其工作人员安全保障的技术性责任与合理使用的应用性责任。事实上，人工智能时代，公共领域个人信息利用的风险主要集中在个人信息的不合理使用情形之下，而确保个人信息安全等技术性责任已形成较为完备的规定，故应着重完善个人信息不合理使用的责任体系，引导规范行政机关对个人信息的合理使用。

（三）完善个人信息主体的损害赔偿制度

无救济则无权利，仅明确行政机关利用个人信息目的与范围、个人信息使用的具体内容、个人信息的利用方式及责任形态等尚显不足。个人信息保护的制度体系中，我们还需完善个人信息权益侵害的救济制度，实现个人信息保护的完整闭环。如前所述，现行法对行政机关利用个人信息着重关注对个人信息的安全保障，并课以相应的行政责任甚至刑事责任，《民法典》对此也作进一步强调。但《民法典》将个人信息的相关权益定位成人格权益而无法适用现行《国家赔偿法》的有关规定。实践中，囿于国家机关泄漏、滥用个人信息，造成有关信息主体人身或财产损失的案例屡见不鲜，但信息主体作为真正的受害人，其个人信息权益的损害却无从救济。

对此，立法者与学界也给予了足够的关注，如《个人信息保护法（草案）》2017 年版中指出：“国家机关违反本法规定，给信息主体造成人身或财产上的损失的，应依照本法的规定承担损害赔偿等民事责任；本法无规定的，依照《中华人民共和国国家赔偿法》的规定承担民事责任。”[24]笔者认为，将民事责任引入政府的侵权责任之中，并承认行政机关侵害个人信息责任的竞合是一种有效的保护路径。一方面，正在制定的《个人信息保护法》应明确国家机关对个人信息侵权的民事责任、行政责任及刑事责任，实现与《民法典》第 999 条等条款之衔接；另一方面，也可以通过完善《国家赔偿法》对个人信息侵害的赔偿规则，完善赔偿范围和标准，从而适应人工智能时代智慧治理中个人信息侵权的新样态。需要强调的是，在智慧治理场景中，个人信息的主要风险更集中于行政机关对个人信息的滥用，造成对相关信息主体的歧视与不当限制等精神损害。因此，在修改完善《国

家赔偿法》的一般人格权赔偿范围时，我们应重点配套完善精神损害赔偿规则，除“赔礼道歉、消除影响或者恢复名誉”等法定义务外，侵权人对被侵权人还应承担精神损害赔偿责任。

五、结语

基于数据的智慧政府正逐渐推动政府治理向人工智能精准治理的范式转变，公民个人信息等数据成为智慧政府治理社会、公共服务的重要资源。然而，智慧治理并不仅是新技术在社会治理中的直接应用，更是对社会治理和法治秩序的颠覆和重建。为此，党的十九届四中全会也明确提出：“要建立健全运用互联网、大数据、人工智能等技术手段进行行政管理的制度规则。”[25]个人信息在社会治理场景中如何被利用便是其中亟待解决的重大课题。《民法典》针对公民个人信息在人格权编予以专门保护，就个人信息的范围、个人信息所蕴含的价值及其权利（权益）属性予以确认，为规范行政机关合理利用个人信息提供指引。通过制定行政机关对个人信息合理使用的规则体系，明确行政机关的技术性责任与应用性责任的双重责任形态，完善行政机关侵害个人信息主体的损害赔偿制度，在制度设计层面实现政府在智慧治理中合理利用个人信息的目的。当然，人工智能技术的迅猛发展决定了智慧治理系统中个人信息分析工具可能随时突破法律事先预设的界限。为此，智慧治理的创新发展与规制不仅要重视智慧治理的顶层设计，还需加强法律规则在系统开发中的嵌入，以技术手段识别违法收集、使用个人信息的行为，进而实现个人信息的技术保护。

参考文献：

[1]张新宝.从隐私到个人信息:利益再衡量的理论与制度安排[J].中国法学,2015,(3)

[2]林鸿潮.个人信息在社会风险治理中的利用及其限制[J].政治与法律,2018,(4).

[3]胡忠惠.大数据时代政府对个人信息的保护问题[J].理论探索,2015,(2).

[4]赵宏.从信息公开到信息保护:公法上信息权保护研究的风向流转与核心问题[J].比较法研究,2017,(2).

[5]黄顺.8万“治安高危人员”被清出深圳[N].深圳商报,2011-04-11(A5).

[6]宋华琳，孟李冕.人工智能在行政治理中的作用及其法律规制[J].湖南科技大学学报（社会科学版）,2018,(6).

[7]张永生，孙贝贝.漩涡中的睢宁政府版征信[N].新京报,2014-07-02(A14).

[8]孙清白,王建文.大数据时代个人信息“公共性”的法律逻辑与法律规制[J].行政法学研究,2018,(3).

[9]肖登辉,张文杰.个人信息权利保护的现实困境与破解之道——以若干司法案例为切入点[J].情报理论与实践,2017,(2).

[10]陈晓勤.公共行政领域中的个人信息保护[J].法学杂志,2013,(10).

[11]Zeynep Tufekci.Algorithmic Harms beyond Facebook and Google:Emergent Challenges of Computational Agency,13J.on Telecomm.& HighTech.L.203(2015).

[12]孙建丽.算法自动化决策风险的法律规制研究[J].法治研究,2019,(4).

[13]程啸.论我国民法典中的个人信息合理使用制度[J].中外法学,2020,(4).

[14]周汉华.探索激励相容的个人信息治理之道——中国个人信息保护法的立法方向[J].法学研究,2018,(2).

[15]程啸.民法典编纂视野下的个人信息保护[J].中国法学,2019,(4).

[16]周汉华.中华人民共和国个人信息保护法(专家建议稿)及立法研究报告[M].北京:法律出版社,2006.

[17]习近平.充分认识颁布实施民法典重大意义,依法更好保障人民合法权益[J].求是,2020,(12).

[18]王利明.论人格权保护的全面性和方法独特性——以《民法典》人格权编为分析对象[J].财经法学,2020,(4).

[19]刘权.论网络平台的数据报送义务[J].当代法学,2019,(5).

[20]陈俊秀.大数据时代个人信息“合理使用”制度研究——以2011-2017年公布的773份刑事判决书为研究样本[J].大连理工大学学报（社会科学版）,2019,(3).

注释：

1 参见《中共中央关于坚持和完善中国特色社会主义制度,推进国家治理体系和治理能力现代化若干重大问题的决定》，新华网，http://www.qstheory.cn/yaowen/2019-11/07/c_1125202003.htm。

2 参见《中华人民共和国民法典》第1035条。

3 天网工程是中央政法委牵头，公安部、工信部等相关部委共同发起建设的信息化工程，实现城市治安防控和管理。其主要由GIS地图、图像采集、传输、控制、显示和控制软件等设备组成，对固定区域如交通要道、治安卡口、公共聚集场所、宾馆、学校、医院以及治安复杂场所安装视频监控设备进行实时监控和信息记录，各种类型的视频监控设备又被称为“天眼”系统。参见《2000万摄像头看着你的天网工程侵犯隐私了吗？》，中国青年网，https://news.china.com/domesticgd10000159/20170929/31528539.html。

4 参见《身份证漏洞帮了犯罪分子的忙》，中国人大网：http://npc.people.com.cn/n/2013/0821c14576-22636564.html。

5 参见《社会信用体系建设调查:是“道德绑架”还是“诚信创新”？》，中国政府网，http://www gov.cn/xinwen/2014-06/19/content_2703960.htm。

6 参见《多地政府网站泄露贫困户个人隐私信息,公示标准有待统一》，光明时评，https:/guancha.gmw.cn/2018-04/29/content_28558983.htm。

7 如齐爱民、周汉华、张新宝等学者先后分别提出不同版本的个人信息保护法的建议稿。参见：齐爱民《中华人民共和国个人信息保护法学者建议稿》(《河北法学》2019年第1期)，周汉华《中华人民共和国个人信息保护法(专家建议稿)及立法研究报告》(法律出版社,2006年版)，张新宝、葛鑫《个人信息保护法(专家建议稿)》，https://civillaw.com.cn/gg/t/?id=36127#。

8 本文通过无讼法律数据库以“个人信息”“个人隐私”等为关键词进行全文检索统计，具体结果如表1所示。

9 通说认为，个人信息知情权是个人信息主体权利制度中的一项基本制度,尽管有明文规定的法律文件较少,但多数涉及个人信息处理的相关法律法规或多或少地均蕴含了知情权的权利内涵。

10 参见:《中华人民共和国统计法》第 9 条，《中华人民共和国政府信息公开条例》第 15 条。

11 参见:《中华人民共和国个人身份证法》第 19 条，《统计执法监督检查办法》第 46 条，《食品药品监督管理统计管理办法》第 25 条，《刑法修正案(九)》第 17 条第 2 项，等等。

12 关于个人信息的权益属性，存在“人格权”“财产权”等多种不同认识。参见：王利明《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》(《现代法学》2013 年第 4 期)，杨立新《个人信息:法益抑或民事权利——对〈民法总则〉第 111 条规定的‘个人信息’之解读》(《法学论坛》2018 年第 1 期)，程啸《民法典编纂视野下的个人信息保护》(《中国法学》2019 年第 4 期)，刘德良《个人信息的财产权保护》(《法学研究》2007 年第 3 期)，龙卫球《数据新型财产权构建及其体系研究》(《政法论坛》2017 年第 4 期)。

13 参见《中华人民共和国国家赔偿法》第 2、3、35 条。

14 参见王利明《〈民法典〉为治理现代化提供有力的制度保障》，光明网，https://theory.gmw.cn2020-07/07/content_33963626.htm。

15《民法典》就个人信息的处理范围、判断标准、处理原则等作出基础性规定。参见《中华人民共和国民法典》第 111、1034、1035 条。

16 如张新宝认为,政府不能无节制地肆意收集和利用个人信息,个人信息法律保护制度的发展始终伴随着对政府权力的限制;王利明也指出,个人信息是一项受法律保护的利益,它不仅需要得到其他民事主体的尊重,也需要国家公权力机构予以尊重。参见：张新宝《从隐私到个人信息:利益再衡量的理论与制度安排》(《中国法学》2015 年第 3 期)，王利明《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》(《现代法学》2013 年第 4 期)。

17 参见:《日本个人信息保护法》第 1 条，中国法学网，http://www.iolaw.org.cn/showNews.aspx?id=12426;《台湾个人资料保护法》第 1 条。

18 参见《中华人民共和国民法典》第 1036 条。

19 参见王晨《关于〈中华人民共和国民法典(草案)〉的说明——2020 年 5 月 22 日在第十三届全国人民代表大会第三次会议上》,中国人大网，http://www.npc.gov.cn/npc/c30834/20200550c0b507ad32464aba87c2ea65bea00d.shtml。

20《宪法》和原《土地管理法》都规定,为公共利益的需要,可以依法对土地实行征收并给予补偿,但何为公共利益一直没有明确界定。新的《土地管理法》创造性地对土地征收的“公共利益”进行了明确界定,列举了为公共利益可以依法征收集体土地的 6 种情形。参见《中华人民共和国土地管理法》第 45 条。

21 参见《中华人民共和国民法典》第 1038 条第 1 款。

22 参见《中华人民共和国民法典》第 1038 条第 2 款。

23 参见《中华人民共和国民法典》第 999、1038、1039 条。

24 参见齐爱民《中华人民共和国个人信息保护法学者建议稿》(《河北法学》2019 年第 1 期)。

25 参见《中共中央关于坚持和完善中国特色社会主义制度,推进国家治理体系和治理能力现代化若干重大问题的决定》，新华网，http://www.xinhuanet.com/politics/2019-11/05/c_1125195941htm。