Dispute Settlement 争议解决, 2025, 11(7), 104-112
Published Online July 2025 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2025.117220

Hans汉斯

自动化行政中个人信息的法律保护研究

闫皓玥

青岛科技大学法学院，山东 青岛

收稿日期：2025年6月9日；录用日期：2025年7月6日；发布日期：2025年7月15日

摘　要

在信息技术飞速发展的当下，自动化行政已深度融入现代社会治理，显著提升了行政效率与公共服务水平。然而，伴随而来的是个人信息在收集、存储、使用和共享等环节面临严峻风险。个人信息作为公民的核心权益，不仅关系到个人隐私与人格尊严，在数字化社会经济活动中也占据关键地位。自动化行政对个人信息的广泛运用，虽推动了行政管理现代化，但信息泄露、滥用等问题频发，严重威胁公民合法权益，甚至可能引发社会信任危机。鉴于此，深入探究自动化行政中个人信息的法律保护极具现实意义。通过研究，有助于填补法律空白，完善我国个人信息保护法律体系，为公民信息安全提供坚实法律保障。同时，能够有效规范自动化行政行为，平衡行政效率与个人信息保护之间的关系，促进自动化行政健康、可持续发展，维护社会公平正义与稳定。

关键词

自动化行政，个人信息保护，法律完善

Research on the Legal Protection of Personal Information in Automated Administration

Haoyue Yan

Law School, Qingdao University of Science and Technology, Qingdao Shandong

Received: Jun. 9th, 2025; accepted: Jul. 6th, 2025; published: Jul. 15th, 2025

Abstract

In the era of rapid development of information technology, automated administration has deeply integrated into modern social governance, significantly enhancing administrative efficiency and the level of public services. However, along with this comes the severe risks that personal information faces in the processes of collection, storage, use, and sharing. As the core right of citizens, personal information not only relates to personal privacy and dignity but also holds a crucial position in

文章引用: 闫皓玥. 自动化行政中个人信息的法律保护研究[J]. 争议解决, 2025, 11(7): 104-112.
DOI: 10.12677/ds.2025.117220

digital social and economic activities. While the extensive application of personal information in automated administration has promoted the modernization of administrative management, problems such as information leakage and abuse occur frequently, seriously threatening the legitimate rights and interests of citizens and even potentially triggering a crisis of social trust. In light of this, in-depth exploration of the legal protection of personal information in automated administration is of great practical significance. Through research, it can help fill legal gaps, improve China's legal system for personal information protection, and provide a solid legal guarantee for citizens' information security. At the same time, it can effectively regulate the behavior of automated administration, balance the relationship between administrative efficiency and personal information protection, promote the healthy and sustainable development of automated administration, and maintain social fairness, justice, and stability.

Keywords

Automated Administration, Personal Information Protection, Legal Improvement

1. 引言

随着信息技术的迅猛发展，自动化行政在现代社会治理中扮演着愈发关键的角色。自动化行政凭借其高效、精准的特点，极大地提升了行政效率，优化了公共服务供给，为社会的有序运行提供了强大助力。然而，在这一过程中，个人信息的大量收集、存储、使用与共享，使得个人信息面临前所未有的风险。

个人信息作为公民的重要权益，不仅关乎个人的人格尊严与隐私安全，更在数字化时代的社会经济活动中具有重要价值。自动化行政系统对个人信息的广泛运用，虽推动了行政管理的现代化进程，但信息泄露、滥用、非法交易等问题也接踵而至，严重威胁到公民的合法权益，甚至可能引发社会信任危机。

在此背景下，深入研究自动化行政中个人信息的法律保护具有极其重要的现实意义。一方面，这有助于填补法律在该领域的空白与漏洞，完善我国个人信息保护的法律体系，为公民个人信息筑牢法律屏障。另一方面，能够规范自动化行政行为，平衡行政效率与个人信息保护之间的关系，促进自动化行政的健康、可持续发展，维护社会的公平正义与稳定。因此，对自动化行政中个人信息法律保护的研究迫在眉睫，刻不容缓。

2. 自动化行政与个人信息保护的理论阐释

2.1. 自动化行政概述

在当今数字化浪潮的席卷下，自动化行政作为一种新兴的行政模式正逐渐崭露头角。它是行政领域与现代信息技术深度融合的产物，以人工智能、大数据、云计算等前沿技术为依托，旨在提升行政效率、优化公共服务。自动化行政的核心在于利用自动化设备或电子技术，按照预设的程序、算法，对行政事务进行智能化处理，从而实现部分或全部行政流程的自动化运作。

从内涵来看，自动化行政涵盖了信息的收集、存储、传输、分析乃至决策执行等各个环节。以智能交通管理系统为例，遍布城市道路的摄像头实时捕捉车辆行驶信息，这些海量数据瞬间传输至数据中心，经过智能算法的快速分析，自动识别交通违法行为，并即时生成处罚指令，整个过程无需人工逐一干预，

极大地提高了执法效率。这不仅体现了技术对行政流程的重塑，更凸显了自动化行政精准、快速的优势[1]。基于其功能与运行机制，可将自动化行政系统细分为数据驱动型、算法决策型和流程自动化型三大类。

数据驱动型自动化行政系统以海量数据的收集与分析为基础。以智能交通管理系统为例，遍布城市道路的摄像头实时捕捉车辆行驶信息，这些数据瞬间传输至数据中心。其特点在于能够快速处理和整合多源异构数据，通过数据分析模型挖掘潜在规律，为行政决策提供依据。然而，这类系统存在数据安全与隐私泄露风险。大量包含个人行踪、行为习惯等敏感信息的数据一旦被非法获取或滥用，将严重侵犯公民隐私权。此外，数据质量参差不齐也可能导致分析结果偏差，影响行政决策的准确性。对此，应建立严格的数据访问权限管理机制，采用加密技术保障数据传输与存储安全，同时加强数据质量监管，定期对数据进行清洗与校验。

算法决策型自动化行政系统着重于通过算法对行政事务进行判断和决策。如行政审批中的“秒批”系统，只要申请人符合既定条件，系统便严格依照预设算法迅速批准。其优势在于减少人为干预，确保决策的公平性与一致性，提高行政效率。但算法黑箱问题是其主要风险点，不透明的算法可能导致决策缺乏可解释性，公众难以理解决策依据，进而引发对行政公正性的质疑。同时，算法偏差可能导致歧视性决策，损害特定群体利益。针对这些问题，需建立算法公开与审查机制，要求行政机关对涉及公共利益的算法进行公开说明，接受社会监督；引入第三方机构对算法进行定期评估，及时发现并纠正算法偏差。

流程自动化型行政系统致力于实现行政流程的全自动化操作，像税务部门的电子报税系统，纳税人在线提交申报信息后，系统自动审核、计算税额，快速反馈结果。该系统的特点是标准化程度高、执行效率快，能有效减少人工操作失误，提升行政服务质量。不过，系统稳定性和可靠性面临挑战，一旦出现技术故障或系统漏洞，可能导致整个行政流程停滞，影响公共服务的正常供给。此外，过度依赖自动化流程可能削弱行政人员的专业判断能力。为降低风险，应建立完善的系统备份与容灾机制，定期进行系统维护与升级，同时加强行政人员培训，使其在必要时能够进行人工干预和应急处理。

自动化行政具有鲜明的特征。其一，高度自动化是其最显著的标志。传统行政依赖人工操作，难免受限于人力的效率与精度，而自动化行政借助智能技术，能在瞬间处理海量数据，完成复杂任务，如税务部门的电子报税系统，纳税人在线提交申报信息后，系统自动审核、计算税额，快速反馈结果，大大缩短办税时间。其二，标准化程度高。预设的程序和算法确保每一个行政行为都遵循统一的规则和标准，减少人为因素导致的差异与偏差，像行政审批中的“秒批”系统，只要申请人符合既定条件，系统便严格依照标准迅速批准，保障了公平性与公正性。其三，高效化贯穿始终。快速的数据处理能力使行政决策和服务得以即时响应，无论是应急管理中的灾害预警与资源调配，还是公共服务领域的社保福利发放，自动化行政都能以最快速度落实，满足社会需求。

展望未来，自动化行政将朝着更加智能化、人性化的方向发展。一方面，人工智能技术的进阶将赋予行政系统更强的自主决策能力，使其能够应对复杂多变的现实情境，提供精准定制化的服务；另一方面，随着公众对数字服务体验要求的提升，自动化行政将更加注重用户需求，优化交互界面，确保技术与人文关怀相得益彰，推动政府治理效能迈向新台阶。

2.2. 个人信息的界定与分类

个人信息作为自动化行政中的关键要素，其精准界定与合理分类是构建有效保护体系的基石。依据我国《个人信息保护法》，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，不包括匿名化处理后的信息。这一法律界定明确了个人信息的核心特征——可识别性，即无论是直接标识信息，如姓名、身份证号、手机号码等，还是准标识信息，像性别、出生日期、

职业等，只要能在特定情境下锁定特定自然人，皆属于个人信息范畴。

从分类维度审视，个人信息依据不同标准呈现多元类别。按照敏感度划分，可分为敏感个人信息与一般个人信息。敏感个人信息涵盖生物识别信息、宗教信仰、特定身份信息、医疗健康信息、金融账户信息等，此类信息一旦泄露，极易对个人的人格尊严、人身安全与财产权益造成严重侵害[2]。例如，人脸信息、指纹信息等生物识别数据，具有唯一性与不可变更性，一旦被非法获取，个人身份极易被盗用，引发诸如诈骗、冒名顶替等违法犯罪行为；又如医疗健康信息，关乎个人隐私与生命健康，不当披露可能导致患者遭受歧视、就业受限等困境。而一般个人信息，虽敏感度相对较低，但同样承载个人生活轨迹与社交印记，如网络浏览记录、购物偏好等，大量汇聚后经数据分析也可能勾勒出个人全貌，存在隐私泄露风险。

基于用途差异，个人信息又可归类为身份认证信息、服务提供信息、行为分析信息等。在自动化行政场景下，身份认证信息用于核实行政相对人身份，确保行政行为指向精准无误；服务提供信息辅助行政机关依据个人需求调配资源、提供定制化公共服务；行为分析信息则助力洞察社会趋势、优化行政决策，然而，若缺乏严格管控，这些信息在收集、存储、传输、使用各环节都可能偏离正轨，使个人权益暴露于风险之中。明确个人信息的界定与分类，为后续探讨自动化行政中个人信息保护的边界与重点筑牢根基，指引法律规制精准发力。

2.3. 自动化行政中个人信息保护的理论基础

自动化行政中个人信息保护根植于深厚的理论土壤，这些理论基石为构建严密的保护体系提供了坚实支撑。

宪法人格尊严理论首当其冲，是个人信息保护的核心依据。宪法作为国家根本大法，将人格尊严奉为公民基本权利的价值原点。个人信息作为承载人格特征、生活轨迹、内心意愿的关键载体，与人格尊严紧密相连。在自动化行政的复杂流程里，个人信息被海量收集、深度分析，一旦泄露或被不当使用，个体将毫无隐私可言，沦为“透明人”，尊严扫地。例如，在智能安防系统中，若人脸信息、出行数据等肆意流出，个人行踪随时被曝光，生活安宁被打破，公众场合的安全感荡然无存，这无疑是对人格尊严的粗暴践踏。宪法保障人格尊严，内在要求对个人信息实施严格保护，确保个人在数字时代依然能掌控自身信息命运，维持独立、自主、受尊重的人格状态[3]。

公共利益本位理论亦不容忽视。行政活动本质是以公共利益为导向，旨在增进社会福祉、维护公共秩序。自动化行政作为行政手段革新，虽追求高效治理，却不能以牺牲个人信息权益为代价[4]。一方面，个人信息合理运用能助力公共利益实现，如疫情防控期间，精准收集居民健康信息、行程轨迹，经科学分析可为防控决策提供有力依据，保障公众生命健康安全，推动社会有序运转；另一方面，若忽视个人信息保护，过度采集、滥用信息引发公众信任危机，反而阻碍行政效能提升，损害公共利益根基。因而，在自动化行政进程中，需精准权衡个人信息保护与公共利益获取，以公共利益为本位，优化个人信息处理规则，实现二者动态平衡，让自动化行政在法治轨道上稳健前行，切实服务社会大众。

责任政府理论同样为个人信息保护保驾护航。政府作为公权力执掌者，肩负保障公民权利、维护社会公平正义的重任[5]。在自动化行政领域，政府主导各类信息系统建设与运行，大量经手个人信息。基于责任政府理念，政府有义务从信息收集源头把关，遵循合法、正当、必要原则，杜绝过度收集；在信息存储、传输、使用各环节，构筑严密安全防线，防范数据泄露；面对信息主体的诉求，及时响应，赋予查询、更正、删除等权利，对信息处理失当行为担责。当出现如社保信息泄露、政务数据违规共享等侵害个人信息事件时，政府必须迅速彻查、严肃追责，以实际行动彰显责任担当，重塑公众信任，确保自动化行政中的个人信息处于安全可控境地，切实服务于人民对美好生活的向往与追求。

3. 自动化行政中个人信息面临的法律风险

3.1. 过度与违规信息收集

在自动化行政蓬勃发展的进程中，信息收集作为起始环节，却暗藏诸多风险，过度收集与违规收集问题尤为突出，给个人信息安全蒙上阴影。

以智慧政务平台为例，部分地方政府为追求管理的精细化、服务的精准化，在政务 APP 或线上办事系统中过度索取个人信息。民众在办理诸如公积金查询、社保业务等常规事项时，除基本身份信息外，还常被要求提供大量非必要信息，像详细的家庭成员信息、社交账号信息等。一些政务 APP 的权限申请更是肆无忌惮，动辄要求获取用户的地理位置、通讯录、相册等权限，远远超出业务办理实际所需范畴，使得民众在享受政务便利的同时，被迫让渡大量个人隐私，个人信息随时面临被滥用的风险。

“天网工程”作为维护公共安全的重要手段，在全国范围内构建起严密的视频监控网络，为打击犯罪、保障社会稳定立下汗马功劳。然而，在其建设与运行过程中，个人信息保护的隐忧也逐渐浮现。一方面，海量摄像头遍布大街小巷，在未经充分告知公众并取得明确同意的情况下，不间断地捕捉行人面部特征、行踪轨迹等敏感信息，公众几乎处于全程“被监视”状态，个人隐私空间被极大压缩；另一方面，视频监控数据的存储、传输缺乏足够的加密与访问管控措施，一旦遭遇黑客攻击或内部人员违规操作，极易造成信息大规模泄露，给公众带来不可估量的安全隐患，个人信息保护与公共安全保障之间的平衡亟待重塑。

3.2. 信息存储与传输存在漏洞

信息存储与传输环节宛如自动化行政的“大动脉”，支撑着数据的流转与运用，然而，此环节却饱受安全漏洞隐患的困扰，为个人信息保护拉响警报。

诸多自动化行政系统在开发时，因对系统安全架构设计的前瞻性不足，致使各类漏洞频出。部分政务数据存储平台，在搭建过程中未充分考虑数据的加密存储需求，采用较为薄弱的加密算法甚至明文存储，一旦遭遇黑客攻击，个人信息便如“裸奔”般暴露无遗。以某市社保信息系统为例，其存储的海量参保人员姓名、身份证号、社保账户金额等敏感信息，因系统漏洞被黑客轻易攻破，导致信息大规模泄露，给参保民众带来极大困扰，诈骗电话纷至沓来，个人财产安全岌岌可危。

网络攻击更是存储与传输环节的“心腹大患”。在全球化网络互联互通的当下，自动化行政系统置身于复杂多变的网络环境，面临着来自四面八方的威胁。分布式拒绝服务攻击(DDoS)可瞬间使系统瘫痪，阻断信息传输通道，让行政服务陷入停滞；恶意软件入侵则悄然在系统内潜伏，伺机窃取、篡改个人信息，如臭名昭著的“WannaCry”勒索病毒，曾肆虐全球，不少政务机构的电脑中招，存储其中的未加密个人信息惨遭加密勒索，若不支付赎金便面临永久丢失风险，严重影响行政工作正常开展与民众权益保障。

加密技术应用的短板同样不容忽视。部分自动化行政场景下，数据传输过程未采用符合安全标准的加密协议，如在一些基层政府部门的数据报送环节，因未启用安全套接层协议(SSL)或传输层安全协议(TLS)，信息以明文形式在网络中穿梭，极易被网络嗅探工具截获；即便采用了加密措施，若密钥管理不善，如长期使用固定密钥、密钥存储缺乏安全防护，也会为黑客破解加密提供可乘之机，使得个人信息在存储与传输途中“风雨飘摇”，安全防线脆弱不堪。

3.3. 信息使用与共享滥用

信息使用与共享环节作为自动化行政的关键流程，一旦脱离法治轨道，极易滋生滥用与失控风险，对个人信息权益造成严重冲击。

在行政机关内部，部分工作人员受功利主义驱使，存在违规使用个人信息的现象。一些基层干部利用职务之便，擅自查询公民个人信息，用于非公务目的，如满足个人好奇心、为亲友提供便利等，致使个人信息在行政体系内“暗流涌动”，隐私泄露风险骤升。在某起案例中，一名户籍民警违规查询并泄露居民个人信息，被不法分子利用实施诈骗，给当事人造成巨大经济损失，公众对行政机关的信任也因此蒙上阴影。

随着自动化行政的推进，行政机关与第三方机构的信息共享日益频繁，这无疑为信息滥用撕开了一道口子。部分商业机构打着“大数据分析”“精准服务”的幌子，在与行政机关共享信息后，肆意挖掘个人信息的商业价值，全然不顾信息主体的意愿与权益。例如，一些保险公司从交通管理部门获取车主信息后，未经车主同意，频繁拨打推销电话，强行推送保险产品，严重干扰个人生活安宁；更有甚者，个别不良企业在获取政务数据中的个人信息后，将其与自身商业数据整合，进行精准“画像”，实施价格歧视，违背市场公平原则，让消费者在毫不知情中沦为“待宰羔羊”，个人信息的合理使用边界在商业逐利中被肆意践踏，亟待法律重筑防线，勒紧信息使用与共享的“缰绳”，守护个人信息安全净土。

4. 自动化行政中个人信息法律保护的完善建议

4.1. 构建完善的法律规范体系

面对自动化行政中个人信息保护的诸多挑战，构建完善的法律规范体系迫在眉睫，这是筑牢个人信息安全防线的基石。

一方面，应进一步细化个人信息保护的相关规则。在信息收集环节，明确规定行政机关及相关主体必须遵循“最小必要”原则，精准界定收集目的、范围与方式，杜绝随意扩大收集范畴[6]。例如，办理社保业务时，仅可收集与社保权益核定直接相关的身份、就业、参保信息，禁止额外索取无关的社交、消费等信息；同时，要求以清晰、易懂的方式向信息主体告知收集详情，获取其明确同意，保障信息主体知情权与选择权。在信息存储与传输环节，制定严格的加密标准与安全防护规范，强制要求采用先进加密算法对个人信息加密存储，如政务数据存储平台应采用国密算法，确保数据保密性；传输过程必须启用安全套接层协议(SSL)或传输层安全协议(TLS)，并定期更新密钥，防止信息被窃取或篡改。在信息使用与共享环节，严格限定使用目的与共享范围，行政机关内部建立审批流程，防止工作人员擅自挪用信息；与第三方共享时，签订详尽的保密协议，明确信息使用边界，确保第三方在约定范围内合理利用信息，违反规定则施以重罚，以严密规则规范信息流转全流程。

另一方面，加快制定政务数据共享、算法监管等专项规范。在算法监管方面，我国可系统借鉴国外经验构建具体监管框架与标准：分层分类立法监管，可参照欧盟《人工智能法案》的风险分级逻辑，将自动化行政中的算法分为三类规制。首先是高风险算法，涵盖社保待遇核定、行政处罚等直接影响公民基本权利的场景，强制要求通过第三方算法审计并公开决策逻辑。如德国《算法问责法》要求社保算法需披露年龄、收入等特征变量的权重系数，我国可规定此类算法上线前需向省级网信部门提交《算法可解释性报告》，并在政务平台公示核心决策规则。其次是中风险算法：如政务服务“秒批”系统，需落实算法备案与定期评估制度。可借鉴美国 NIST《AI 风险管理框架》的迭代机制，要求行政机关每季度对算法偏差率进行测试，此经验可用于我国公务员招录自动化系统的监管。还有低风险算法：如政务 APP 的智能客服，可实行自我声明合规制，但需嵌入用户投诉接口，当投诉量超过一定阈值时触发临时审查。政务数据共享规范应明确不同部门间数据共享的条件、流程与安全保障措施，构建统一的数据共享平台，实施分级分类共享机制，既促进数据流通助力行政效能提升，又防止敏感信息无序扩散。例如，公安、民政、税务等部门共享人口基础信息时，通过数据中台进行脱敏、加密处理后按权限定向共享，保障数据可用性与安全性。算法监管规范要着力解决算法黑箱问题，要求算法设计者对算法逻辑、数据来源、

决策机制进行详细备案，监管部门定期审查，确保算法公正、透明，避免算法歧视、偏见导致个人信息被不当处理。同时，引入第三方专业机构进行算法评估，为算法合规性背书，一旦发现算法违规操作致使个人信息受损，及时责令整改、追究责任，以专项规范为自动化行政中的个人信息保护“保驾护航”。

此外，在相关法律法规中增设行政公益诉讼条款，将自动化行政中个人信息保护纳入行政公益诉讼受案范围[7]。当行政机关违法处理个人信息，侵害不特定多数人权益，且常规监督手段失效时，检察机关有权提起行政公益诉讼，督促行政机关纠正违法行为，修复受损公益。这犹如高悬的“达摩克利斯之剑”，强化对行政权力的监督制约，为个人信息保护提供坚实的司法后盾，填补法律救济短板，全方位守护个人信息安全，推动自动化行政在法治轨道上稳健前行。

4.2. 强化行政机关的保护责任与监督机制

行政机关作为自动化行政的主导者与执行者，在个人信息保护中肩负着不可推卸的核心责任，强化其保护责任与监督机制是守护个人信息安全的关键环节。

一方面，需进一步明确行政机关在个人信息处理各环节的具体保护职责。在信息收集阶段，严格要求行政机关遵循法定程序，依据“最小必要”原则精准确定收集范围，杜绝盲目扩大信息索取边界。例如，民政部门在办理社会救助业务时，仅收集申请人家庭经济状况、人口结构等直接关联救助资格审核的信息，不得额外收集无关的个人社交细节、消费偏好等信息；同时，要确保告知义务落实到位，以通俗易懂的方式向信息主体阐明收集目的、用途、存储期限及信息主体享有的权利，取得其明确同意，切实保障信息主体的知情权与选择权。在信息存储与传输环节，行政机关应建立高标准的安全防护体系，采用先进的加密技术、入侵检测与防范系统，对存储设备、传输通道进行全方位监控与防护[8]。如税务部门的征管系统，对纳税人的申报信息、完税记录等敏感数据，运用国密算法加密存储，并实时监测数据传输链路，及时预警、阻断非法入侵行为，确保数据在存储与传输过程中的机密性、完整性。在信息使用与共享环节，建立严格的内部审批流程，明确使用目的限定，防止工作人员擅自挪用信息谋取私利；与第三方共享信息时，不仅要签订严谨细致的保密协议，还需对第三方的信息使用情况进行全程跟踪监督，确保信息流向可控、用途合规，一旦发现违规行为，立即终止共享并追究责任。

另一方面，构建严密的监督机制不可或缺。在行政机关内部，设立专门的个人信息保护监督小组，定期对各部门的信息处理工作进行全面审查，包括信息收集的合规性、存储的安全性、使用的正当性等方面，审查结果纳入绩效考核体系，与部门绩效、个人奖惩挂钩，促使工作人员强化信息保护意识[9]。同时，拓宽外部监督渠道，鼓励公众积极参与监督举报。建立便捷高效的举报平台，开通专门热线、网络举报入口等，方便公众在发现个人信息被不当处理时能够及时反馈；对公众举报线索进行及时核实、处理，并将处理结果公开透明，增强公众信任；此外，引入第三方专业机构进行独立评估，借助其专业技术与客观视角，对行政机关的个人信息保护工作成效进行周期性测评，提出改进建议，形成内外协同、多元共治的监督格局，全方位督促行政机关守牢个人信息保护防线，为自动化行政的健康发展营造安全有序的环境。

4.3. 加强信息主体的权利赋能与救济途径

在自动化行政的复杂架构下，强化信息主体的权利赋能与疏通救济途径是保障个人信息权益的关键环节，二者相辅相成，共同为个人信息安全保驾护航。

一方面，应全方位赋予信息主体更多权利。知情权首当其冲，行政机关及相关信息处理者在收集个人信息时，必须以清晰、明确、易懂的方式告知信息主体收集目的、用途、存储期限、共享范围以及信息主体所享有的各项权利，确保信息主体对自身信息的流向与运用了如指掌。例如，在公民办理电子政务

业务时，通过弹窗提示、专门说明页面等形式，详细阐释每一项信息收集的缘由与后续处置安排，杜绝含糊其辞、晦涩难懂的告知条款，让信息主体真正做到心中有数。更正权同样不可或缺，当信息主体发现自身信息存在错误、遗漏或过时等情况，应有权便捷、高效地向信息处理者提出更正申请，信息处理者需在规定期限内完成核查与更正流程，确保信息的准确性与时效性。如个人在社保信息系统中发现自己的就业经历、参保年限记录有误，可通过线上专门渠道提交更正诉求，社保部门迅速响应核实，及时修正错误信息，避免因错误信息导致权益受损。

另一方面，疏通多元救济途径迫在眉睫。行政救济层面，优化行政复议流程，针对自动化行政中个人信息纠纷的特殊性，选拔配备兼具法律专业知识与信息技术素养的复议人员，建立快速审查机制，缩短复议周期，提高复议效率。当信息主体对个人信息处理行为不服提起复议时，复议机关能迅速切入问题核心，精准判断信息处理的合法性、合理性，及时纠正不当行为，为信息主体提供及时有效的救济。司法救济维度，完善行政诉讼制度，明确举证责任分配规则，鉴于信息主体在证据获取上的弱势地位，要求行政机关对自动化行政系统的算法逻辑、数据处理流程、信息存储状况等关键证据承担主要举证责任，打破信息不对称壁垒[10]；同时，加强司法人员的专业培训，定期组织涉及自动化行政与个人信息保护的专题培训，提升司法裁判人员对复杂技术问题的理解与判断能力，确保在诉讼中能准确认定侵权事实、合理衡量损害赔偿，为信息主体撑起司法维权的“保护伞”，让个人信息保护在法治轨道上落地生根，切实维护信息主体合法权益。

5. 结论

通过对自动化行政内涵、特征及发展趋势的梳理，明晰其在提升行政效能、优化公共服务方面的巨大潜力，同时揭示出个人信息在这一进程中面临的诸多风险挑战。从信息收集环节的过度与违规收集，到存储传输环节的安全漏洞隐患，再到使用共享环节的滥用失控风险，乃至信息主体权利保障面临的救济困境，层层递进地展现出个人信息保护形势的严峻性。

在理论层面，宪法人格尊严、公共利益本位、责任政府等理论为个人信息保护筑牢根基，彰显保护个人信息在维护个体尊严、平衡公共利益、督促政府履职方面的重大意义。实践层面，提出构建完善法律规范体系，细化规则、制定专项规范、引入公益诉讼；强化行政机关保护责任与监督机制，明确职责、内外监督协同；加强信息主体权利赋能与救济途径，赋予多元权利、疏通复议诉讼救济渠道等一系列针对性建议，力求全方位、多层次构建个人信息保护屏障，确保自动化行政在法治轨道上稳健前行。

展望未来，随着技术持续迭代升级，自动化行政将深度融入社会治理各领域，个人信息保护研究需紧跟时代步伐。一方面，应深化跨学科研究，融合法学、计算机科学、社会学等多学科知识，攻克算法监管、隐私增强技术应用等难题，以技术创新赋能法律保护；另一方面，国际合作研究有待加强，在全球化数据流动背景下，借鉴国际先进经验，协同构建跨境个人信息保护规则，应对跨国数据处理挑战，切实保障个人信息权益，为数字时代政府治理现代化与个人权利保障的双赢局面不懈努力。

参考文献

[1] 陈飏, 裴亚楠. 论自动化行政中算法决策应用风险及其防范路径[J]. 法学, 2021(1): 75.

[2] 孙清白. 敏感个人信息保护的特殊制度逻辑及其规制策略[J]. 行政法学研究, 2022(1): 119-130.

[3] 马颜昕. 数字政府: 变革与法治[M]. 北京: 中国人民大学出版社, 2021: 361-362.

[4] 查云飞. 行政裁量自动化的学理基础与功能定位[J]. 行政法学研究, 2021(3): 114-124.

[5] 叶必丰. 行政法的人文精神[M]. 北京: 北京大学出版社, 2005: 114-115.

[6] 黄学贤. 行政法中的比例原则研究[J]. 法律科学, 2001(1): 72-73.

[7] 孔祥稳. 论个人信息保护的行政规制路径[J]. 行政法学研究, 2021(1): 131-145.
[8] 敖双红. 论自动化行政及其法律规制[J]. 湖南警察学院学报, 2017(1): 84-85.
[9] 展鹏贺. 数字化行政方式的权力正当性检视[J]. 中国法学, 2021(3): 114-116.
[10] 李晴. 自动化行政处罚何以公正[J]. 学习与探索, 2022(2): 72-81.