

行政机关匿名信息大数据处理的法律规制

王正鑫

摘要：大数据技术可基于相关关系挖掘，从匿名信息集合中获取公共行政管理与服务活动所需的知识内容。匿名信息大数据处理虽不指向具有识别性的个人，但会侵犯行政管理对象的私密信息、促成行政权力技术性扩张以及弱化行政决策的情景要素，因而存在法律规制必要性。既有法律规范在规制匿名信息大数据处理方面存在功能短板，并主要体现为未将匿名信息纳入调整范围、强调个体导向而缺失群体关怀，以及正当必要原则难以容纳大数据处理的全样本模式。匿名信息大数据处理的法律规制要求对既有信息处理规则进行调整，即个人信息概念应纳入群体保护理念、确立公共利益目的限制原则并提升大数据处理过程的透明度。

关键词：匿名信息；大数据处理；个人信息；群体保护

〔中国分类号〕D922.1 〔文献标识码〕A 〔文章编号〕2096-6180(2025)04-0104-18

引言

公共行政管理与服务活动的有效实施得益于信息资源的充分掌握，行政权力行使过程本身就是信息收集、分析和利用的过程。^{〔1〕}行政机关根据职权行使的需要，尽可能多地收集、分析和利用各类信息，并在此基础上形成执法决策、作出行政行为，对公民权利义务进行处理。由于行政机关的信息处理活动蕴含权力要素，并会连带影响公民、法人和其他组织的合法权益，因此也需要遵守信息处理规则。在《中华人民共和国个人信息保护法》（下称《个人信息保护法》）所确立的制度框架下，信息被区分为个人信息与非个人信息，并与宽严程度不同的信息处理规则相匹配。个人信息包含身份识别标识，凸显人格特征，与人格利益息息相关^{〔2〕}，以之为对象的信息处理活动因关乎人格尊严而须受到严格的法律约束。而非个人信息因为无法关联至特定个人，立法预设

〔作者简介〕王正鑫，法学博士，北京航空航天大学博士后在站研究人员。

〔基金项目〕国家社会科学基金项目“数字政府的法治化建构研究”（项目批准号：24VRC041）。

〔1〕林鸿潮：《个人信息在社会风险治理中的利用及其限制》，载《政治与法律》2018年第4期，第5页。

〔2〕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》，载《现代法学》2013年第4期，第69-70页。

非个人信息处理活动仅具有较低的权益侵害风险,相关法律制度也以激励信息流通利用为主旨。⁽³⁾在此基础上,行政机关的个人信息处理活动会受到严格的法律制约,而非个人信息处理活动则受钳制较少。

偏重个人信息处理的法律规制模式具有合理性,同时也与个人信息保护的现实需要相契合。个人信息作为个人识别标识而与行政管理对象直接相关,可以直观反映行政管理对象的守法与违法情况,无须深度分析即可成为事实认定的证据来源。信息泄露、隐私侵犯等法律风险也主要存在于个人信息处理中,对个人信息处理施加严格法律规制可以有效规范行政权力,保护行政管理对象的合法权益。但是,伴随数字政府建设的持续推进,行政机关开始借助大数据技术完成规模化信息集合的智能处理。不同于传统的信息处理方式,大数据技术并不关注个人信息所包含的身份标识,其致力于从海量信息中提取一般规律,挖掘共性价值。⁽⁴⁾换言之,大数据技术以群体为目标,并不关注可识别的个人身份。这意味着,即便对个人信息进行匿名化处理,大数据技术也可以从信息集合中提取具有利用价值的分析结论⁽⁵⁾,如违法犯罪行为人的—般特征、暴力犯罪高发的时空条件。这些有价值的信息将成为行政权力的行使基础,为执法决策提供重要参考,如对具有违法犯罪特征的人进行针对性询问,对可能发生违法犯罪行为的区域加强巡视。

需要承认的是,伴随数字技术融入公共行政管理与服务活动,行政机关的信息处理模式正在发生变化,信息处理重心正在从个人信息转向非个人信息,基于大数据技术的匿名信息处理将愈发重要。匿名信息大数据处理为行政机关规避严苛的个人信息处理规则提供了可能,行政机关可以绕过本应履行的个人信息处理义务,较为自由地处理非个人信息,从中获取执法决策所需的信息资源。这会给围绕个人信息构建的法律制度带来根本冲击,个人信息处理规则将可能被架空。行政机关可以借助匿名化操作规避个人信息处理规则的约束,同时也无碍于信息处理目标的达成。⁽⁶⁾问题也随之而来,当行政机关的信息处理模式发生转变,是否有必要对匿名信息大数据处理施加法律规制?如有必要,适宜的法律规制方案又应如何选择?为解答前述问题,笔者先基于大数据技术的实践应用,归纳匿名信息大数据处理的基本模式,然后指出将匿名信息大数据处理纳入法律规制的必要性,最后阐述适宜的法律规制路径。

(3) 这方面的立法例以欧盟《非个人数据自由流动条例》为代表。Free Flow of Non-Personal Data Regulation: Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union, OJ 2018 L 303/59.

(4) 张凌寒:《算法权力的兴起、异化及法律规制》,载《法商研究》2019年第4期,第67页。

(5) Jennifer Jiyoung Suh et al., *Distinguishing Group Privacy from Personal Privacy: The Effect of Group Inference Technologies on Privacy Perceptions and Behaviors*, 2 Proceedings of the ACM on Human-Computer Interaction 1, 2 (2018); Alessandro Mantelero, *Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection*, 32 Computer Law & Security Review 238, 246 (2016).

(6) 个人信息经匿名化或去标识化后便不再属于个人信息,这可以有效规避个人信息保护规则。在不影响信息处理效果的前提下,信息处理者倾向于对个人信息进行匿名化或去标识化操作。参见[荷]玛农·奥斯特芬:《数据的边界:隐私与个人数据保护》,曹博译,上海人民出版社2020年版,第63页。

一、匿名信息大数据处理的基本模式

在以往,由于匿名信息不直接关联至行政管理对象,难以在违法犯罪防控、公共福利分配、行政审批登记等方面发挥作用,因此行政机关缺失处理匿名信息的内在动力。然而,匿名信息虽不能直接表征行政管理对象的健康状态、行踪轨迹、性格特征等身份标识,但也蕴含着丰富的信息内容,具有支撑行政权力行使的巨大潜力,只不过囿于传统信息处理手段,匿名信息的潜在价值难以被充分挖掘。以大数据、人工智能为代表的数字技术正在打破信息处理的技术局限,匿名信息大数据处理正是随着数字技术发展而出现的新型信息处理模式,其已在公共行政管理与服务活动中受到广泛应用。在讨论是否有必要对匿名信息大数据处理施加法律规制之前,尚需要对这一新型信息处理模式进行机理剖析,指出其与传统信息处理模式的不同之处,以便为后续论述预作铺垫。基于公共行政管理与服务的实践需要,匿名信息大数据处理可适用于多个场景,如违法犯罪预测、个人和企业征信评级、行政辅助决策等。虽然适用场景具有多元化,但不同场景中的匿名信息大数据处理遵循着相似的技术逻辑,即借助相关关系挖掘,从原始信息集合中析取新知识,并将新知识应用于公共行政管理活动。

(一) 基于相关关系挖掘新知识

信息收集是信息处理的前提,只有尽可能多地收集信息,才能为后续挖掘信息价值提供足够的原始物料。借助数字技术手段,自动化、大范围、持续性的信息收集已不受人力和时空条件的限制,再加之行政机关之间的跨部门信息归集,行政机关得以汇聚海量的信息集合。⁽⁷⁾然而问题在于,初始收集的信息类型多样,格式杂乱,其中还混杂着重复、错误的信息内容,尚不能直接用于执法决策,因此通过信息收集所聚拢的原始信息并不具有较高的利用价值。大数据技术可以对散乱、庞杂的原始信息进行深度挖掘,从中提取有价值的规律、隐藏的模式等新知识。⁽⁸⁾经过大数据技术的深度挖掘,原本潜藏于原始信息中的新知识将浮出水面。就技术原理而言,大数据技术挖掘的新知识建立在相关关系之上,即“存在于两个或多个数据集合之间的关系,识别出有用的关联物,进而揭示事物中某些属性同时出现的规律和模式”。⁽⁹⁾在技术层面,相关关系属于数理关系,是基于数理计算所得的概率推论,考察两种或多种事物之间的对应关系,实践应用价值在于透过此现象了解彼现象。⁽¹⁰⁾正是基于相关关系的挖掘,大数据技术可以从历史信息中萃取出辅助行政决策的知识内容。以预测警务为例,基于对过往违法犯罪案件的深度挖掘,对未来特定区域、特定时段发生的违法犯罪行为进行预测,以便采取针对性的侦防策略和警力布控。⁽¹¹⁾

(7) 郑晓军:《反思公共数据归集》,载《华东政法大学学报》2023年第2期,第54页。

(8) 闫铁鑫:《大数据背景下预测型警务的构建》,载《犯罪研究》2018年第2期,第18-19页。

(9) 彭知辉:《基于大数据的警务预测:局限性及其顺应之道》,载《中国人民公安大学学报(社会科学版)》2016年第2期,第39页。

(10) 栾兴良:《大数据侦查观的反思与重构》,载《中国刑警学院学报》2021年第6期,第6页。

(11) 杨青春:《海安:“大数据+”巡防模式提升街面警务战斗力》,载《人民公安报》2024年3月25日,第3版。

需要说明的是,虽然大数据技术可以从原始信息中挖掘何种内容无法预知,但基于大数据技术的信息处理往往有着目标导向,这些信息处理的目标导向服务于特定的公共行政管理和服务目的。基于信息处理目标导向的不同,大数据技术从原始信息集合中提取的新知识也有不同的内容表现,如具有较高违法犯罪风险的行为特征、引发群体事件的社会矛盾类型、恶性传染病的区域流行特点等。但是这些新知识均是原始信息集合未曾记录的知识,也是无法通过因果关系等已知逻辑推理手段获取的知识。换言之,大数据技术所挖掘的新知识不是对原始信息的简单归总,而是对原始信息的深度转化,其以原始信息为加工物料,从中萃取出原始信息无法直接表达的有价值信息。更为重要的是,新知识的获取需要挖掘原始信息的潜藏价值,是从整个信息集合中提取的公因式般的一般规律或者共性特征。这意味着,原始信息集合是否包含个人信息并不必要,因为新知识的获取非但不关注具有识别性的个人身份标识,反而需要跳脱出个人信息所承载的个性化特征。换言之,大数据技术看重原始信息集合构成的“整体”,而非个人信息所彰显的“个体”。在此基础上,基于大数据技术的信息处理可以摆脱个人信息处理规则的钳制,同时亦可以达成行政机关所预设的信息处理目标。

(二) 新知识的实践应用

信息处理并非止步于获取新知识,将新知识应用于公共行政决策才是其最终目的所在。原始信息集合经过大数据技术的洗礼而被转化为新知识,并最终落地为行政权力运行的事实基础。从海量原始信息中提取的新知识可以有效打破信息偏差、缩减信息盲区,一定程度上能够减少决策失误,优化决策质量并提高决策效率。基于公共行政决策需求的不同,新知识的实践应用较为多元,既可以被用于不针对特定行政管理对象的通用型决策,如预测犯罪高发区域并将之作为部署警力、加装视频监控设备的决策根据,也可被用于针对特定行政管理对象的个别化决策,如对行政管理对象个人进行违法犯罪风险判断,并据此决定是否对其展开进一步的侦查措施。新知识的实践应用,本质上是大数据技术提取的一般规律应用于公共行政管理活动。这背后遵循着“模式匹配”原则,即将待解决的公共行政管理事项与大数据技术提取的一般规律进行比对。如果公共行政管理事项能被涵摄入大数据处理所提取的一般规律,那么即可基于一般规律作出行政决策。^[12]例如,借助大数据技术提取吸毒人员在年龄、性别、有无固定居所等方面的共有特征,作为行政管理对象是否存在吸毒嫌疑的判断标准。若某一行政管理对象满足前述特征,则会被识别为潜在的吸毒人员。^[13]

需要注意的是,新知识的实践应用并不必然涉及个人信息。一方面,不针对行政管理对象个人的通用型决策并不指向特定行政管理对象,无需个人信息即可完成。通用型决策往往具有普遍适用性,强调覆盖范围的广泛性,如制定行政规范性文件、发布行政指导、部署技术监控设施。

[12] Rainer Mülhlof, *Predictive Privacy: Collective Data Protection in the Context of Artificial Intelligence and Big Data*, 10 Big Data & Society 1, 2 (2023).

[13] 刘绪崇等编:《智慧警务:大数据环境下新时代公安信息化建设模式探索》,清华大学出版社2018年版,第36页。

另一方面,针对行政管理对象个人的执法决策虽然需要个人信息,但也仅在实践应用阶段发挥作用,新知识的挖掘阶段并不需要个人信息。例如,公安机关盘问具有违法犯罪嫌疑的行政管理对象,便需要获取行政管理对象的个人信息,从而精准识别其是否属于违法犯罪行为人。但是,大数据技术从原始信息集合中所提取的违法犯罪特征并不建立在个人信息之上,而且由于新知识是从已存在的原始信息集合中提取的,这相当于将过往的历史信息作为现在或未来的决策基础。因此,新知识的实践应用意味着行政权力运行的事实基础正在发生改变,即行政机关不再基于当前的公共行政管理事项进行回应性信息获取,而是根据已往的历史信息集合构筑行政权力行使的事实基础。可以说,匿名信息大数据处理不单单表征一种信息处理模式,还因嵌入行政决策而变革行政机关的决策方式。这意味着匿名信息大数据处理会在公共行政管理与服务活动中扮演愈加重要的角色,成为行政决策不可或缺的信息基础。匿名信息大数据处理如图1所示。

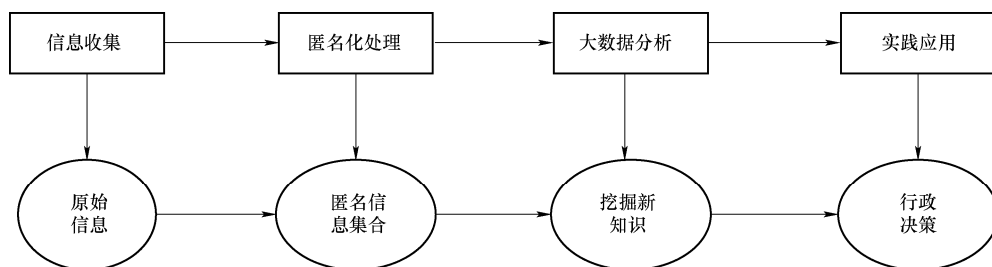


图1 匿名信息大数据处理图

二、匿名信息大数据处理的法律风险

前已提及,基于大数据技术的信息处理并不需要个人信息的参与即可完成目标任务。当个人信息经由匿名化、去标识化操作而成为匿名信息后,以之为对象的信息处理活动便与个人信息无关。在世界范围内,主流的立法模式均将信息处理活动的法律规制重点瞄准个人信息,以个人信息为对象的信息处理活动需要受到严格的法律约束,如遵循知情—同意原则、信息处理目的应合法正当等。与此同时,个人信息主体被立法授予查阅权、更正权和可携带权等一系列权利内容,其可以对个人信息处理活动施加控制。^{〔14〕}反观匿名信息,《个人信息保护法》明确将匿名信息排除出调整范围^{〔15〕},匿名信息处理者得以逃逸严格的法律约束。在比较法层面,以欧盟为代表的个人信息保护立法《通用数据保护条例》(General Data Protection Regulation, GDPR)更是围绕个人信息构筑起一系列信息处理规则。立法对个人信息和匿名信息的区别对待暗含立法者的价值判断,即匿名信息处理对法秩序的负面影响较小,没有法律规制的必要性。然而,大数据技术的新近发展打破了这一立法预设,匿名信息大数据处理对法秩序的威胁不亚于个人信息的处理。而且,行

〔14〕 姚佳:《个人信息主体权利的实现困境及其保护救济》,载《中国法律评论》2022年第6期,第136—137页。

〔15〕 《个人信息保护法》第4条第1款。

政机关匿名信息大数据处理所引发的负面影响极具复杂性，其不但会侵犯行政管理对象的合法权益，还会对依法行政原则产生威胁。

（一）侵犯行政管理对象的私密信息

私密信息主要存在于个人的私生活领域，是个人不希望为外界所知的隐秘一隅。依照《中华人民共和国民法典》（以下简称《民法典》）第1032条第1款的规定，基于隐私权的规范效力，任何组织或者个人不得刺探、侵扰、泄露和公开他人的私密信息。通常情况下，对私密信息的获取以对个人私生活领域的物理入侵为前提，并体现为前述《民法典》所言的刺探、侵扰、泄露和公开等侵犯手段。在此基础上，私密信息完全处于个人的自主控制之下，个人可主动决定是否对外公开私密信息。然而，大数据技术可以打破个人对其私密信息的自主控制，私密信息不再单纯属于私生活领域的隐秘角落。大数据技术的应用价值在于从原始信息集合中提取新知识，这些新知识基于相关关系挖掘得来，属于难以直接获取的推论性信息。大数据技术的这一优势使得行政机关可以从易于获取的普通信息中推算出难以获取的信息，其中就包括行政管理对象通常不为外人所知的私密信息。比如，借助社交媒体用户留存于网络的行为信息，大数据技术可以从中提取出性生活、生理特征乃至隐晦疾病的识别规律，继而将之用于推测行政管理对象的私密信息。^{〔16〕}行政机关无须与行政管理对象直接接触，就能够规避法律对敏感个人信息获取的苛刻要求^{〔17〕}，取得私人领域中最为隐秘的信息。这为行政机关深度入侵行政管理对象的私人领域开辟了便利通道，在不对私人领域进行物理入侵的前提下，就可以不着痕迹、悄无声息地揭露私人领域的隐秘一隅。

更为严峻的是，不管单个行政管理对象对自身私密信息采取多么谨慎的管理措施，均不敌大数据技术获取私密信息的能力优势。原因在于，大数据处理中的私密信息不是从特定个人身上提取的，而是从他人提供的信息集合中推测出来的。而且，即便对来自他人的信息集合作匿名化处理，大数据技术也可以从中提取私密信息。^{〔18〕}换言之，个人私密信息是否被他人得知不再取决于自身，而是取决于同作为社会成员的他人向行政机关提供了何种内容以及多少数量的信息。^{〔19〕}可以认为，大数据技术使得私密信息可以与个人私生活领域相剥离，对私密信息的探知也无须依托刺探、侵扰、泄露和公开等传统的物理入侵方式。这将颠覆传统的私密信息获取模式，并导致行政权力向私人领域的无限扩张。因为行政管理对象无法通过个人信息权益、隐私权等权利保护机制捍卫自身的私密信息，行政机关可以通过尽可能多地收集与行政管理对象相关的各类信息，通过匿名化操作规避个人信息处理规则和隐私权保护规则，然后将之用于推测其想获知的私密信息，

〔16〕 Michele Loi & Markus Christen, *Two Concepts of Group Privacy*, 33 *Philosophy & Technology* 207, 221 (2020).

〔17〕 相较于一般个人信息，《个人信息保护法》对敏感个人信息处理施加了更为严格的限制，即具有特定目的和充分的必要性，并采取严格保护措施，同时须遵守更为严格的“知情—同意”规则。参见《个人信息保护法》第28—31条。

〔18〕 Lanah Kammourieh et al., *Group Privacy in the Age of Big Data*, in Linnet Taylor, Luciano Floridi & Bart van der Sloot eds., *Group Privacy: New Challenges of Data Technologies*, Dordrecht: Springer, 2017, p. 65.

〔19〕 Rainer Mülhlof, *Predictive Privacy: Collective Data Protection in the Context of Artificial Intelligence and Big Data*, 10 *Big Data & Society* 1, 7–8 (2023).

从而达成公共行政管理与服务目的。公共领域与私人领域之间的边界会因此淡化甚至消弭，将国家绝缘于个人自治领域之外的公法设想将会落空。

（二）辅助行政权力技术性扩张

在依法行政的法治框架下，行政权力源自立法授权，明确且有限。若着眼于行政权力的行使效能，受限于人力短板、时空范围等现实因素，则源自立法授予的行政权力并不能被完全行使。例如，行政机关难以查处所有的道路交通违法行为，无法向所有生活困难的行政管理对象支付最低生活保障金。所以说，行政权力内容的实现程度受制于现实条件，会因现实条件的限制而打折扣。然而，数字技术可被用于置换权力，提升行政权力的行使效能。在数字技术的助力下，行政机关得以突破物理时空、人力短板、物质资源等诸多限制，“治理的范围、对象、手段等方面的边界或数量得以大大拓展”。^{〔20〕}这在大数据处理中体现得尤为明显，在前大数据时代或称小数据时代，信息资源匮乏、信息收集缓慢且成本高昂，信息收集只能局限于随机性的样本选择。大数据技术强化了行政机关的信息处理能力，稀松平常的信息汇聚后也能产生饱含价值的新知识，辅助行政机关完成行政决策。信息处理活动不再囿于人力，也不再止步于经验性的简单推理，大数据技术可以完成信息集合的深度分析，充分获取信息的潜藏价值。得益于此，行政机关得以实施先前所不能为之事，如违法犯罪预测、企业违规行为智能监管、行政审批智能化办理。伴随信息处理能力的增强，行政机关的权力内容和权力边界也在不断扩张。

不同于立法授予的行政权力，基于大数据技术攫取的权力内容脱离了民主立法程序的正当性检验，本质上属于行政机关依托数字技术开辟的权力空间。这种权力内容可能与立法授予的行政权力相关，如具有行政立法权的行政机关可基于大数据技术优化行政立法内容。^{〔21〕}但也有可能凌驾于立法授予的行政权力之上，如行政机关利用大数据技术生成的执法规则篡改上位法律规范。^{〔22〕}因此，大数据技术开辟的权力空间并不必然与行政机关的法定职权相一致。数字技术可以优化行政权力的行使条件，也可以帮助其逃逸立法控制。而且，由于不同地域、层级、职能的行政机关在大数据技术应用能力方面存在明显差异，所以有技术应用优势的行政机关将成为强势部门，甚至可以获取原由其他行政机关行使的权力，这无疑会在组织法层面上破坏行政系统内部的职权分配。^{〔23〕}

行政权力的技术性扩张会对依法行政原则产生威胁，并会危及行政机关与立法机关之间的宪法分工。为对行政权力施加有效控制，立法机关从组织法层面和行为法层面设置法律规则，从而为行政权力行使树规立矩。在组织法层面，行政机关的权力来源需要恪守职权法定原则，即行政

〔20〕 施伟东：《论市域社会治理数字化转型的法治推进》，载《政治与法律》2022年第3期，第95页。

〔21〕 刘佳明：《人工智能立法的运用及其规制》，载《湖南农业大学学报（社会科学版）》2021年第1期，第57-58页。

〔22〕 王正鑫：《“立法性”算法权力的兴起与法律规制》，载《法制与社会发展》2023年第2期，第196-198页。

〔23〕 梅立润：《技术置换权力：人工智能时代的国家治理权力结构变化》，载《武汉大学学报（哲学社会科学版）》2023年第1期，第47页。

权力源自宪法和组织法授予。立法在向行政机关授予权力的同时，也对行政权力内容作出相对明确的界定，从而起到对行政权力的控制作用。⁽²⁴⁾在行为法层面，源自立法授权的行政权力不能放任行政机关自由行使，而应遵循立法机关预先设定的实体和程序要件。以行政处罚实施为例，只有在应受行政处罚行为满足构成要件该当性，并且行政机关依法履行说明理由、听取陈述、申辩等法定程序步骤的前提下，行政处罚行为方能满足合法性要求。行政权力的技术性扩张使得行政机关可以通过数字技术实现自我赋权，在立法授权的边界之外开辟权力行使空间。行政机关实际行使的权力内容不再局限于立法授权，而更偏向于数字技术所能容许其行使的权力内容。就此，依法行政有转向依技术行政的风险，依法行政原则会被架空悬置，立法机关作为行政权力授予机关的宪法角色亦会受到冲击。

（三）削减行政决策的情景化要素

大数据技术服务于信息的规模化收集、深度分析与智能应用，塑造数字化场景并促成公共行政管理活动的自动化和智能化转型。基于行政权力的行使需要，大数据技术对粗糙的原始信息集合进行加工，从中挖掘出原始信息难以表达的新知识。这些新知识将为行政权力行使提供事实基础乃至决策辅助。需要说明的是，经由大数据技术生成的知识内容与物理世界中的现实状况有所差异，其不是对现实状况的数字化等价转换，而是可量化、可计算的技术构造物。基于此，公共行政管理活动将转向数字虚拟化，行政决策的情景化要素被严重削减，并具体表现为以下三个方面。

其一，行政管理对象不再是活生生的自然人，而是大数据技术构建的数字人。这些数字人是由大数据技术基于信息集合构建出来的，即从信息集合中提取行政管理对象的群体特征，然后将行政管理对象设定为满足群体特征的个体。⁽²⁵⁾这样的数字身份不仅与物理世界中的个人身份相脱离，即“与特定的个人、他们的主观性和生活经验相分离”⁽²⁶⁾，而且会因大数据处理模型参数的调整而不断发生变化⁽²⁷⁾。这会导致行政管理对象的虚拟化，并错位于物理世界中行政管理对象的真实状况。当行政机关面向行政管理对象作出决策时，需要充分考虑行政管理对象的实际情况，如违法情节、年龄、语言能力等具体因素，并在此基础上作出个别化的情景式决策。如果行政机关以大数据技术构造出的虚拟行政管理对象为决策对象，其决策内容会因脱离具体情景而失真。

其二，大数据技术可以塑造行政决策的事实基础。这里存在两个层面的事实建构：第一层是对历史信息集合的加工，目的在于形成可被量化计算的标准化事实；第二层是以历史信息中提取

(24) 应松年：《完善行政组织法制探索》，载《中国法学》2013年第2期，第20页。

(25) Luciano Floridi, *Group Privacy: A Defence and an Interpretation*, in Linnet Taylor, Luciano Floridi & Bart van der Sloot eds., *Group Privacy: New Challenges of Data Technologies*, Dordrecht: Springer, 2017, p. 113–115.

(26) [荷]马克·舒伦伯格、[荷]里克·彼得斯编：《算法社会：技术、权力和知识》，王延川、栗鹏飞译，商务印书馆2023年版，第41页。

(27) Linnet Taylor, *Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World*, in Linnet Taylor, Luciano Floridi & Bart van der Sloot eds., *Group Privacy: New Challenges of Data Technologies*, Dordrecht: Springer, 2017, p. 32.

的标准化事实为参照，将之用于当下或未来状况的事实确认。因而，大数据技术生成的决策结果不是基于当下的事实状况，而是基于当下事实与过去事实的相关性。以预测警务为例，大数据技术可以从过往违法犯罪案件中抽取违法犯罪行为高发的天气、时间、季节等事实特征，然后将之用于违法犯罪行为预测。^{〔28〕}

其三，大数据技术输出的决策内容属于技术层面的数理计算结果，而非规范层面的法律适用结果。大数据处理机制是受制于模型参数，并被用于调整辅助变量与目标变量之间关系的数学函数。在此基础上，行政决策是基于数理计算得出的“最优解”，而不是根据个案事实得出的唯一法律效果判断。大数据模型参照过去类似案例的处理结果，分析输入信息与输出信息之间的关联性，然后选择相关性最强的处理结果。然而问题在于，相关性最强的处理结果并不等同于符合法律适用的“最优解”。事实情节的细微变化、法律规范的更新改动均会对法律适用结果产生影响，历史性的经验归纳不能完全预测未来的事物状态。

可以看到，借助大数据技术，行政决策的作用对象、事实基础和决策方式均出现不同维度的数字化。行政机关不再单单从物理世界的行政管理对象处调查事实、寻找法律规范并作出法律效果判断。来自行政管理对象的行为数据，即便是匿名化的，大数据技术也可以从中提取出数字化的行政管理对象、创造出可量化计算的事实，并通过数理计算确定具有概率相关性的决策结果。公共行政管理活动中的个案情景化决策不再是唯一的决策模式，其存在空间会因大数据技术与行政权力的深度融合而被不断压缩。但是，当个案情景化决策不再重要，围绕个案情景化决策所设计的行政权力合法性控制机制将无法被妥帖适用，实体处理的合法适当性、行政权力行使程序的法定性、基于行政裁量所生的个案正义均会湮没于大数据技术所营造的数字虚拟环境中。

三、既有法律体系的制度缺陷与功能短板

匿名信息大数据处理会侵犯行政管理对象的私密信息，促成行政权力的技术性扩张，并削减行政决策的情景化要素，弱化行政决策的规范理性。这表明匿名信息大数据处理会对法秩序带来负面影响，因而存在法律规制的必要性。需要追问的是，前述负面影响能否被现行法律规范所消解？换言之，匿名信息大数据处理能否在实定法框架下获得有效规制？下文将指出，不管是传统法律框架下的规则设置，还是近些年兴起的个人信息保护立法，均强调个体层面的权利保障而缺失群体层面的规范思维，难以将匿名信息大数据处理纳入调整范围。这导致匿名信息大数据处理游离于法律规制之外，从而与依法行政的法治要求之间存在明显张力。既有法律规范非但无法妥帖适用于匿名信息大数据处理，反而会被架空悬置。

（一）未将匿名信息处理纳入法律规制范围

在比较法层面，1953年生效的《欧洲人权公约》于第8条第1款规定，人人均享有私人和家

〔28〕 杨青春：《海安：“大数据+”巡防模式提升街面警务战斗力》，载《人民公安报》2024年3月25日，第3版。

庭生活、家庭和通信受尊重的权利。在此基础上,欧洲人权法院在 *Leander* 案中确立一项判例法规则,即储存和公开关于私人生活的信息,属于《欧洲人权公约》第 8 条私人生活受尊重权的保护范围。⁽²⁹⁾ 这一判例法规则被之后的判例所承继。⁽³⁰⁾ 通过在个人信息与私人生活之间建立联系,个人信息被纳入《欧洲人权公约》第 8 条的保护范畴。欧盟 1995 年《数据保护指令》第 1 条更是直接强调,自然人的基本权利和自由应受保护,尤其是与个人信息处理相关的隐私权。为加强个人信息的保护力度,在承继 1995 年《数据保护指令》主要内容的基础上,欧盟后又于 2018 年出台《通用数据保护条例》。作为个人信息保护制度构建的先行者,欧洲至迟在 20 世纪 50 年代便已关注个人信息保护的重要性,并展开个人信息保护的实践探索。经过数十年的制度累积,不但在宪法层面确立了个人信息受保护权的基本权利地位,还先后形成了《数据保护指令》《通用数据保护条例》等个人信息保护专门立法。反观非个人信息,非但未受到立法的严格保护,反而以《非个人数据自由流动条例》为代表的法律规范以激励其流动利用为主旨。

在我国法律框架中,匿名信息处理也未受到立法关注。早在 2000 年 12 月 28 日,全国人大常委会就作出《关于维护互联网安全的决定》。其第 4 条强调,“非法截获、篡改、删除他人电子邮件或者其他数据资料”属于犯罪行为。“他人电子邮件或者其他数据资料”主要以个人信息为主,这是立法在以刑事追责的方式强调个人信息保护的重要性。而在 2004 年,全国人大法工委在解释《中华人民共和国宪法》第 40 条时,就基于通信秘密而对国家机关的信息处理活动树规立矩,即移动用户通话详单可以反映公民的通话对象、通话时间等个人隐私和秘密,属于宪法保护的通信秘密。⁽³¹⁾ 移动用户通信资料中的通话详单内容、电子邮件等通信信息通常与公民个人相关联,这其实是借个人隐私保护公民的个人信息权益。至于无法关联至公民个人的匿名信息,包括宪法在内的各级法律规范对其并未述及。及至《个人信息保护法》颁布之后,信息处理规则围绕个人信息而制定。个人信息处理受到法律的严格约束,而匿名信息处理则几乎不受钳制。根据《个人信息保护法》第 4 条第 1 款的规定,个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。这相当于直接宣示,匿名信息处理豁免适用个人信息保护规则。根据当下最新的立法进展,《个人信息保护法》成为个人信息保护领域的专门立法。刑法、民法和行政法三大部门法中也不乏针对个人信息保护的规定⁽³²⁾,但匿名信息处理的规则设置尚付阙如。

可以看到,不管是域外的立法例,还是我国的法律制度,均将个人信息作为法律制度设计的核心。当前风头正盛的个人信息保护制度有着较为久远的制度渊源、周全完善的制度内容。在时

(29) *Leander v. Sweden* [1987] ECtHR 9248/81, para. 48.

(30) *Rotaru v. Romania* [2000] ECtHR 28341/95, para. 43; *S. and Marper v. The United Kingdom* [2008] ECtHR 30562/04, para. 67.

(31) 《全国人民代表大会常务委员会法制工作委员会关于如何理解宪法第四十条、民事诉讼法第六十五条、电信条例第六十六条问题的交换意见》(法工办复字(2004)3号)。

(32) 如 2015 年《刑法修正案(九)》设立侵犯公民个人信息罪;《民法典》(2020 年)于人格权编就个人信息保护作出专门规定;《网络安全法》(2016 年)、《数据安全法》(2021 年)则涉及行政机关的个人信息安全监管任务。

间跨度上,个人信息保护制度的主要内容形成于前大数据时代,这又以1995年欧盟《数据保护指令》为典型。大数据技术的发展、数字时代的到来,凸显出个人信息保护的重要性,并加速个人信息保护制度的立法进程。但是,个人信息保护立法的迭代更新主要是对旧有制度内容的有限调整,仅是小修小补,并未结合大数据技术进行与时俱进的制度革新。以2018年出台的《通用数据保护条例》为例,其基本承继了1995年《数据保护指令》的主要内容,很多条款甚至只字未改。可以说,现有的个人信息保护制度成形于前大数据时代,其中的制度内容也停留在前大数据时代。

然而问题在于,个人信息保护制度虽在其位,却不能承其重。大数据处理会挑战现行个人信息保护规则,并引发亟须解决的法律问题。基于大数据技术的信息处理模式致力于从信息集合中提取一般规律和共性特征,是在信息集合的整体层面而非个体层面进行信息处理。即便对个人信息进行匿名化操作,也无碍于信息处理目标的达成。⁽³³⁾当大数据技术不再关注个人信息,转而在信息集合的整体层面进行知识挖掘,个人信息保护规则的规范效力将限缩为零。因为个人信息保护规则调整是基于个人信息处理所形成的法律关系,匿名信息并不处于个人信息保护规则的效力辐射范围。⁽³⁴⁾如果行政机关借由匿名化操作,将个人信息转变为非个人信息,继而通过大数据技术从中提取新的知识内容,那么围绕个人信息所构筑的信息处理规则将被架空。换言之,围绕个人信息所设置的制度规则已经落后于数字技术的发展步伐,其旧有内容无法满足规制匿名信息大数据处理的需要。

（二）强调个人导向而忽视群体关怀

在传统法律框架下, 制约行政权力、保障公民权利的法律制度设计偏重个人导向, 即将具体且特定的公民个人作为权利救济主体。这主要体现为围绕行政行为所构筑的制约行政权力和保障公民权利的制度框架。行政机关通过作出行政行为来决定特定行政相对人的权利义务内容, 行政复议和行政诉讼制度也主要为具体的行政相对人提供救济。在个人导向的权利保护理念下, 因为匿名信息大数据处理并不涉及具体的行政相对人, 只能被归入内部行政活动并由行政机关自主实施, 其对法秩序带来的负面影响也无从消解。新近兴起的个人信息保护立法强化了权利保护的个人导向, 如《个人信息保护法》第 1 条和第 2 条均开宗明义地规定, 本法以保护自然人的个人信息权益为立法宗旨。《个人信息保护法》所设置的信息处理规则以个人信息权益为基础, 而个人信息权益的受用主体为已识别或可识别的自然人。这表明个人信息保护立法强调个人导向, 将具有识别性的个人作为个人信息处理法律关系的一方主体。在个人导向之下, 个人信息处理者的义务以及个人信息权益的法律救济均须关联至个人, 方有相关法律条款的适用空间。例如, 个人信息主体享有的知情同意权、更正删除权、可携带权等一系列权利, 便是将个人信息处理活动置于

(33) Lanah Kammourieh et al., *Group Privacy in the Age of Big Data*, in Linnet Taylor, Luciano Floridi & Bart van der Sloot eds., *Group Privacy: New Challenges of Data Technologies*, Dordrecht: Springer, 2017, p. 65.

〔34〕 丁晓东：《论个人信息概念的不确定性及其法律应对》，载《比较法研究》2022年第5期，第47页。

个人的控制之下。^{〔35〕}

但对于大数据技术而言，待处理的信息集合是否关联至具有识别性的个人并不重要，其所生成的知识内容也不针对可识别的个人。大数据技术是从信息集合中提取出共性的行为特征，这些行为特征被视作特定群体的身份标识。^{〔36〕} 比如在文旅服务领域，大数据技术可以识别出有潜在文旅服务需求的群体特征，像消费特征、兴趣特征，然后对满足群体特征的对象进行精准的文旅服务信息推送。^{〔37〕} 所以说，大数据技术是从原始信息集合中分析出群体的身份标识，强调对群体身份的数字化构建。^{〔38〕} 因此在大数据处理中，个人的身份标识并不具有独立价值，其需要依附于群体的身份标识，即个人首先作为群体成员而存在，并因成为群体成员而具有群体的身份标签。

在群体视角下，信息处理活动的负面影响首先发生于群体层面，然后才会波及个人。比如在预测警务中，违法犯罪行为的甄别与预测主要基于对海量信息的分析。^{〔39〕} 大数据技术可以分析出具有违法犯罪风险的群体特征，公安机关将据此采取一系列防控措施，如盘问、传唤、拘留满足群体特征的行政管理对象。但受大数据模型参数设置、信息规模与质量等技术因素的影响，对违法犯罪行为的识别预测不可避免地存在误差。^{〔40〕} 行政管理对象可能会被错误识别为违法犯罪行为，从而招致犯罪防控部门的追踪监控。^{〔41〕} 与此同时，大数据处理活动的负面影响虽会波及个人，但不会止步于个人，而是会波及所有符合群体特征的个人。但由于《个人信息保护法》侧重个人导向，其无法提供群体层面的权益保障，仅能为有限的个人提供权益救济。

（三）正当必要原则难以容纳大数据处理

《个人信息保护法》第5条将“正当、必要”确立为个人信息处理的基本原则，有学者将之归为比例原则在个人信息保护领域的具体表现。^{〔42〕} 《个人信息保护法》第19条规定的“个人信息的保存期限应当为实现处理目的所必要的最短时间”、第34条规定的“不得超出履行法定职责所必

〔35〕 林鸿潮：《个人信息在社会风险治理中的利用及其限制》，载《政治与法律》2018年第4期，第4页。

〔36〕 Linnet Taylor, Luciano Floridi & Bart van der Sloot, *Introduction: A New Perspective on Privacy*, in Linnet Taylor, Luciano Floridi & Bart van der Sloot eds., *Group Privacy: New Challenges of Data Technologies*, Dordrecht: Springer, 2017, p. 20.

〔37〕 瞿祥涛：《宜昌市智慧旅游“精准推荐”：满足游客个性化需求》，载《中国文化报》2022年1月25日，第7版。

〔38〕 Luciano Floridi, *Group Privacy: A Defence and an Interpretation*, in Linnet Taylor, Luciano Floridi & Bart van der Sloot eds., *Group Privacy: New Challenges of Data Technologies*, Dordrecht: Springer, 2017, p. 113–115.

〔38〕 Luciano Floridi, *Four Challenges for a Theory of Informational Privacy*, 8 *Ethics and Information Technology* 109, 111 (2006).

〔39〕 胡铭、严敏姬：《大数据视野下犯罪预测的机遇、风险与规制——以英美德“预测警务”为例》，载《西南民族大学学报（人文社会科学版）》2021年第12期，第85–86页；李国军：《论大数据驱动下的预测警务创新》，载《中国人民公安大学学报（社会科学版）》2015年第6期，第4–5页。

〔40〕 刘晓洁、毛欣娟：《侦查视角下人脸识别技术应用研究》，载《山东警察学院学报》2018年第6期，第54页。

〔41〕 Bart van der Sloot, *Do Groups Have a Right to Protect Their Group Interest in Privacy and Should They? Peeling the Onion of Rights and Interests Protected Under Article 8 ECHR*, in Linnet Taylor, Luciano Floridi & Bart van der Sloot eds., *Group Privacy: New Challenges of Data Technologies*, Dordrecht: Springer, 2017, p. 270.

〔42〕 刘权：《论个人信息处理的合法、正当、必要原则》，载《法学家》2021年第5期，第13–15页。

需的范围和限度”，均被认为比例原则在国家个人信息处理活动中受到特别强调。⁽⁴³⁾ 在比例原则之下，个人信息收集应具有特定且合理的目的，满足比例原则的目的正当性要求。⁽⁴⁴⁾ 另外，个人信息收集应遵循“最小侵害原则”，即“无必要不收集”。⁽⁴⁵⁾ 作为一项公法上的基本原则，比例原则可以约束个人信息处理场景中的行政权力，避免个人信息处理活动对行政管理对象权益的不法侵害。就其本质而言，个人信息处理场景中的行政权力主要体现为行政机关的信息处理能力，比例原则所能发挥的约束作用实则在要求行政机关审慎处理行政管理对象的个人信息。

基于正当必要原则的信息处理思维难以适用于匿名信息大数据处理，两者之间的抵牾之处贯穿了整个信息处理过程。在信息收集阶段，匿名信息大数据处理以信息收集为前提，通过多渠道的信息收集，积累起信息分析所需要的目标对象。基于大数据技术的信息处理遵循全样本分析模式，这需要尽可能多地收集信息⁽⁴⁶⁾，因为更多的信息量往往意味着发掘更多新知识的可能性⁽⁴⁷⁾。在信息分析阶段，大数据技术倾向于榨干原始信息的潜藏价值，对其所包含的相关关系进行穷尽式挖掘。⁽⁴⁸⁾ 另外，由于匿名信息大数据处理可以逸脱个人信息保护规则的制约，其也不受限于个人信息处理的目的限制。在数字技术的催动下，物理世界实现了数字化转换，万事万物均可以信息形式存在。这为大数据思维的乌托邦式遐想提供了落地的可能，即海量信息的存在以及越来越多的事物正实现数字化转换。受此促动，行政机关将从个案处理中的信息收集转向常态化、规模化和无差别的信息收集。这样的信息收集模式虽然不限于特定个人，但却将所有行政管理对象涵纳其中。行政机关的信息收集活动将突破个人信息保护立法所确立的正当必要原则，两者属于存一去一的对立关系。对正当必要原则的坚守将阻碍大数据处理的正常开展，对大数据处理的正常开展又会不可避免地违背正当必要原则。

四、匿名信息大数据处理的法律规制路径

匿名信息脱离了个人信息的识别性标签，不再与特定个人相关联。但基于大数据技术的相关关系挖掘，匿名信息集合同样可以被用于生成新知识，为公共行政管理活动提供决策辅助。匿名信息大数据处理昭示了一种全新的信息处理模式，即信息处理目标的达成不以识别个人为前提，而是着眼于信息集合的整体价值。这可以有效提升信息资源的利用效率，显著增强行政机关的信息处理能力。但剑有双刃，匿名信息大数据处理也会对法秩序带来负面影响，而且难以被纳入既有信息处理规则的调整范围。这就要求对既有信息处理规则作出适时调整，为匿名信息大数据处理的法律规制提供规范供给。

(43) 赵宏：《〈民法典〉时代个人信息权的国家保护义务》，载《经贸法律评论》2021年第1期，第15页。

(44) 刘权：《论个人信息处理的合法、正当、必要原则》，载《法学家》2021年第5期，第13页。

(45) 赵宏：《〈民法典〉时代个人信息权的国家保护义务》，载《经贸法律评论》2021年第1期，第15页。

(46) [英] 迈尔·舍恩伯格、库克耶：《大数据时代》，盛杨燕、周涛译，浙江人民出版社2013年版，第41页。

(47) 彭知辉：《基于大数据的警务预测：局限性及其顺应之道》，载《中国人民公安大学学报（社会科学版）》2016年第2期，第39页。

(48) 李国军：《论大数据驱动下的预测警务创新》，载《中国人民公安大学学报（社会科学版）》2015年第6期，第5页。

（一）个人信息概念应纳入群体保护理念

当下的立法聚焦于个人信息，个人信息概念圈定了法律规则的适用范围。个人信息概念中的“个人”指向具有识别性的特定自然人，强调识别性基础上的唯一性。换言之，个人信息保护立法强调个体视角，立足于个人信息权益保护，具有身份识别性的个人是唯一的个人信息权益承载主体。只有以个人信息为对象的信息处理活动才会受到严格的法律制约，以非个人信息为对象的信息处理活动则几乎不受钳制。个人信息与非个人信息僵硬的二元划分所暴露出的制度短板已经引起学界反思。基于个人信息与非个人信息二元区分的制度架构，以及对两者保护力度相差悬殊的规则设置，无法实现对公民权益的周延性保护。^{〔49〕}前述反思在匿名信息大数据处理中获得了印证，侧重个人信息的立法设定在面对大数据技术时显得有些捉襟见肘，难以应对大数据技术的群体面向。大数据技术能够在群体层面对匿名信息集合进行价值挖掘，并将信息处理结果应用于符合群体特征的不特定个人。这是一种面向群体的信息处理模式，不关注具有身份识别性的个人，仅关注经信息聚合而形成的群体以及潜在的群体成员。如果仍然局限于个人信息权益保护的个体视角，个人信息保护的立法目的非但不能实现，反而容易被匿名信息大数据处理侵蚀殆尽，因而有必要树立群体保护理念，将个体放置于群体中进行保护，这是因应大数据技术的权益保护模式。

在大数据处理语境下，个人被一般化为不具有识别性的群体成员，可以是符合群体特征的任何不特定自然人。因此，为保障行政管理对象权益和控制行政机关信息处理权力，有必要对个人信息概念作扩张性解释，将个人信息概念中的“个人”构造为可变的个人，即与信息处理活动有利害关系的不特定个人。经由这一法解释操作，可以将群体保护理念注入信息处理规则，弱化个人信息与非个人信息僵硬的概念区分，避免单纯因概念归属而先验性地划定法律保护强度。个人信息概念的目性扩张解释在法律规范层面也易于操作。个人信息本身是一个内涵与外延均不明确的法律概念，以识别性作为界定基准，通常被立法表述为“与一个已识别或可识别的自然人有关的任何信息”。这一立法界定方式表明，个人信息是一个需要结合特定语境作个别判断的法律概念。^{〔50〕}个人信息概念具有“场景依附性”，“并不存在一个客观的刚性规则，而是取决于识别的目标、被谁识别、识别的概率、识别的风险等多种因素”。^{〔51〕}个人信息概念的不确定性为法律解释提供了操作空间，根据信息权益保护和信息处理权力控制的需要，对个人信息概念作具体场景中的弹性化解释，将与大数据处理活动有利害关系的不特定个人纳入保护范围。

需要强调的是，对个人信息概念的扩张性解释并非毫无边界，而是应慎重处理群体权益保护与个人信息保护立法注重的个人视角之间的关系。具体而言，个人信息保护立法并未预见匿名信

〔49〕 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》，载《环球法律评论》2022年第2期，第85-99页。

〔50〕 欧盟数据保护第29条工作组曾就个人信息概念理解发布意见，认为个人信息的界定须取决于个案的具体情境。Article 29 Working Party, Opinion 4/2007 on the Concept of Personal Data 4/2007, p. 12-16.

〔51〕 丁晓东：《论个人信息概念的不确定性及其法律应对》，载《比较法研究》2022年第5期，第51-52页。

息大数据处理的负面影响,也未将之纳入调整范围。面对迅速发展的信息处理技术,立法的滞后性进一步凸显。若将群体保护理念融入个人信息概念,实则是在延展个人信息保护立法的调整范围,扩充个人信息保护立法的规范对象。这决定了对个人信息概念的扩张性解释只应存在于例外情形,并应出于保护群体权益的目的,而且对群体权益的保护最终仍服务于潜在群体成员即不特定个人的权益保护。在此基础上,当匿名信息大数据处理具有明确的群体指向时,为了保护群体成员的个人权益,才有必要对个人信息概念作扩张性解释,从而将具有权利侵害风险关联性的信息类型纳入个人信息概念范畴,要求匿名信息大数据处理遵循个人信息保护立法的规则设置;而具有较低权利侵害风险或几乎不产生权利侵害风险的信息类型则不被视作个人信息,其流通利用也不应受到过多限制。

(二) 匿名信息大数据处理应遵循目的限制

在大数据时代,不管是个人信息还是匿名信息,均会因反映个人或群体的人格特征而人格化,因成为数字经济生产要素而财产化,所以信息均会在一定程度上关涉人格尊严、人身与财产安全等重要的权利利益。前已提及,行政机关以匿名信息为对象的大数据处理活动也会对相对人的权益产生负面影响。这种负面影响集中体现在揭示私人领域中最为隐秘的信息、掌控数字化人格、削弱行为自由的内在动力等诸多方面。基于此,如果承认行政机关的匿名信息处理行为会深度入侵相对人的私人领域,而且这种深度入侵可以造成相对人权益的实质减损,那么根据公法学的通行观点,对公民权益具有克减效果的公权力行为应受到严格限制。⁽⁵²⁾进一步需要追问的是,应如何对匿名信息大数据处理施加限制,从而避免其对相对人合法权益产生非法侵害呢?

与个人信息不同,匿名信息不与特定个人相关联,这导致知情—同意机制无法发挥作用。行政管理对象并不知晓信息处理情况,行政机关基于何种目的实施信息处理活动完全由其自身主导。尤其大数据技术遵循全样本分析,这促使行政机关进行常态化、规模化和无差别的信息收集,从而保有数量可观的信息集合。这在客观上可以支撑行政机关完成多种目的的信息处理活动,既可以服务于公共行政管理,也有非法滥用的风险。若不对行政机关的匿名信息大数据处理施加目的限制,那么技术赋予的信息处理能力将会演变为难以控制的权力猛兽。为享受数字技术的发展红利,发挥匿名信息大数据处理在公共行政管理与服务活动中的优势效能,就需要弱化匿名信息大数据处理与信息合法、正当使用之间的冲突。这要求行政机关实施的匿名信息大数据处理应出于合法、正当目的,将追求不正当目的的匿名信息处理排除在外。

匿名信息大数据处理的目的限制,指向对匿名信息大数据处理的具体用途进行事前限定。这要求行政机关仅能出于履行法定职责的目的实施大数据处理活动,而且不得超出履行法定职责所必需的范围和限度。目的限制的背后是对行政机关信息处理能力的制约,避免信息处理活动侵犯行政管理对象的合法权益。在立法层面,对于行政机关信息处理活动的目的限制局限于个人信息。

(52) 赵宏:《限制的限制:德国基本权利限制模式的内在机理》,载《法学家》2011年第2期,第153—155页。

《个人信息保护法》第6—7、14条规定，处理个人信息应当具有明确、合理的目的，目的应公开明示，并取得个人同意。匿名信息大数据处理虽不关注具有识别性的个人，但信息处理结果却可以成为行政决策基础，并会影响群体以及群体中的不特定个人，因而仍然有目的限制的必要。由于匿名信息难以适用知情—同意机制，而且单个信息主体的同意也无法代表群体，所以需要另行开辟目的限制的实现方式。

不管是个人信息还是匿名信息处理，行政机关的信息处理活动均存在于特定场景中，即基于公共行政管理的实际需要来获取信息处理结果，典型如预测警务、政务服务智能推荐等。不同场景中的信息处理活动具有高低程度不同的风险，并需要采取强度不同的法律规制举措。^{〔53〕}由于应用场景与信息处理目的相对应，对匿名信息大数据处理的目的限制可以通过应用场景限制来实现。鉴于此，以合理、合法作为判定标准，制定匿名信息大数据处理的应用场景清单，要求行政机关在清单范围内实施匿名信息大数据处理活动，从而在清单中融入匿名信息大数据处理的目的限制要求。^{〔54〕}例如，可以要求公安机关将匿名信息大数据处理专门用于违法犯罪风险预测、串案线索分析等特定执法目的。

（三）提升匿名信息大数据处理的透明度

正当程序原则要求权力拥有者公开权力运行过程，以此证明权力行使的正当性，这需要程序本身公开且程序设计能够避免权力的任意行使。^{〔55〕}但由于匿名信息大数据处理不涉及个人信息，也就无须征求个人信息主体同意、告知信息处理情况。^{〔56〕}这也导致匿名信息大数据处理过程处于行政机关的内部控制，与行政权力依法行使所需的透明度相去甚远，同时也造成行政权力技术性扩张和行政决策情景化要素的缺失。而在制度运行层面来说，对匿名信息大数据处理施加法律规制建立在知晓信息处理情况的基础上，这包括匿名信息集合的内容构成、信息处理目的、信息处理结果等多个方面。因此，若要对匿名信息大数据处理施加有效的法律规制，就需要外化匿名信息大数据处理过程，即提升匿名信息大数据处理的透明度，以便预防或及时阻却侵益性较强的匿名信息大数据处理。

为增强匿名信息大数据处理的透明度，基于既有的学理讨论和制度实践，可以尝试从以下几个方面着手：首先，行政机关应建立匿名信息大数据技术发布机制，公布其所收集的信息类型和使用目的，帮助公众了解信息处理状况。尤其当涉及行政管理对象的私密信息时，行政机关应明确列明私密信息的应用场景。其次，行政机关应如实记录信息处理情况并定期进行影响评估，并就技术漏洞或潜在风险改善信息处理方式，调整大数据模型的参数设置。影响评估应注重技术专

〔53〕 高富平：《个人信息流通利用的制度基础——以信息识别性为视角》，载《环球法律评论》2022年第1期，第84—99页。

〔54〕 Rainer Mühloff, *Predictive Privacy: Collective Data Protection in the Context of Artificial Intelligence and Big Data*, 10 *Big Data & Society* 1, 10 (2023).

〔55〕 陈景辉：《算法的法律性质：言论、商业秘密还是正当程序？》，载《比较法研究》2020年第2期，第130页。

〔56〕 Solon Barocas & Helen Nissenbaum, *Computing Ethics Big Data's End Run Around Procedural Privacy Protections*, 57 *Communications of the ACM* 31, 31—32 (2014).

业性，即交由行业技术专家完成。再次，行政机关应建立信息反馈与纠错机制，激励信息处理活动的利益相关者发现技术漏洞，以便持续优化信息处理活动。最后，需要注意的是，匿名信息大数据处理的透明度并不具有绝对性，国家秘密、商业秘密以及个人隐私依然构成公开豁免理由。若强调匿名信息大数据处理过程的绝对透明，则会削弱行政机关的执法能力、降低执法效率。但只有在法律特别规定的情况下，匿名信息大数据处理才可以被豁免公开，即应遵循法律保留原则。

另外需要强调的是，提升匿名信息大数据处理的透明度可以倒逼行政机关对行政管理对象保持足够的尊重，提醒行政机关不可依仗技术优势而对匿名信息进行没有限度的挖掘。在遵循目的限制的基础上，匿名信息大数据处理仅能在有限的情形下采用，而提升匿名信息大数据处理的透明度能够在一定程度上确保行政机关对目的限制的遵守，避免行政机关追求非公共利益目的。另外，提升匿名信息大数据处理的透明度还可以引导行政机关对其收集的海量信息进行保护性使用，在达成公共行政管理与服务活动目的的基础上，尽量避免对行政相对人造成权益减损的实害化结果。更为重要的是，这一制度设计与匿名信息大数据处理的技术特征相契合，可以有效克服“知情—同意”机制无法适用的困境，同时将匿名信息大数据处理过程予以外化。

五、结语

在现行法律框架下，个人信息受到立法的严格保护，相关制度已经走过数十年的发展历程，经匿名化的非个人信息处理则几乎不受钳制。对个人信息保护的重视源于个人信息与个人身份之间的密切关联，本质上仍可归为对人格尊严等重要法益的制度关怀。伴随数字技术的迅猛发展，个人信息保护问题更加凸显，个人信息保护制度也得以适时更新。但是，数字技术的发展不仅会对个人信息保护产生威胁，还会创生出新的风险源。匿名信息大数据处理是伴随数字技术发展出现的新型信息处理模式，这一信息处理模式颠覆了侧重个人信息的旧有信息处理模式。大数据技术致力于从信息集合中提取群体特征、一般规律或基本模式，信息处理结果的生成不以个人识别为前提，这使得行政机关可以通过匿名化手段规避个人信息保护立法的约束，在摆脱信息处理义务的同时达成信息处理目的。大数据技术支持的匿名信息处理活动虽不针对具有身份识别性的个人，但却会影响匿名信息集合所涉及的群体中的不特定个人，信息处理活动的风险不但未能消弭，反而愈发扩大。这从侧面表明，围绕个人信息所构筑的信息处理规则已经滞后于信息处理技术的发展。行政机关作为一国范围内信息保有量最大的主体，其通过大数据技术获取的信息处理能力需要被纳入法律规制框架，以避免依法行政原则在匿名信息大数据处理场景中落空。

Legal Regulation of Big Data Processing of Anonymous Information in Administrative Organs

WANG Zhengxin

Abstract: Through correlation mining, big data technology can acquire the knowledge content necessary for public administration management and service activities from anonymous information sets. Although the processing of anonymous information by big data does not target identifiable individuals, it will encroach upon the private information of administrative management objects, facilitate the technological expansion of administrative power, and weaken the situational elements of administrative decision-making. Hence, legal regulation is necessary. Current legal frameworks exhibit functional deficiencies in regulating the processing of anonymous information within big data contexts. These shortcomings are primarily manifested in the exclusion of anonymous information from regulatory purview, an overemphasis on individual-oriented approaches at the expense of group considerations, and the principle of legitimacy and necessity failing to align with the comprehensive sample models inherent in big data processing. The legal regulation of the processing of anonymous information by big data requires the adjustment of the existing information processing regulations, namely, the concept of personal information should be integrated into the concept of group protection, the principle of restriction for public interest purposes should be established, and the transparency of big data processing should be enhanced.

Keywords: Anonymous Information; Big Data Processing; Personal Information; Group Protection

(责任编辑: 孔祥稳 汪友年)