个人信息查阅复制权的适用边界与行使机制

李西泠

摘　要：《民法典》与《个人信息保护法》虽已确立个人信息查阅复制权，但在不同处理场景中，该权利的行使状况高度不均衡，规范与实践之间存在明显落差。平台规则、数据控制权配置及技术限制等因素常压缩其适用空间，削弱知情、控制与监督功能。在区分查阅权、复制权与可携带权制度功能的基础上，明确查阅复制权的优先适用地位。通过对电商、社交、企业软件及国家机关等典型场景的分析，揭示该权利的主要受限样态。针对新技术条件下的行使障碍，提出严格审查“技术限制”的正当性，并从请求受理、及时提供及信息可理解性等方面完善行使规则，以推动查阅复制权的实质实现。

关键词：个人信息保护；查阅权；复制权；信息自决；场景化适用

[中图分类号] D922.16；D923　　[文献识别码] A　　[文章编号] 2096-6180 (2026) 03-0117-20

一、问题的提出

在数据主导的现代社会中，信息化程度已达到前所未有的高度，各类服务组织持续、大规模地收集并处理个人信息，并在信息主体难以充分知情或有效理解的情况下，将相关数据广泛纳入算法决策与商业分析过程，尤其用于为广告投放和行为预测提供支持。在此过程中，个人信息逐渐被转化为服务提供者可单方控制和利用的资源〔1〕，信息主体却难以及时、完整地查明其个人信息的具体使用方式与处理逻辑，从而使其对个人信息处理活动的知情、控制与监督能力在实践中不断被削弱。针对上述现实困境，我国立法已通过确立个人信息查阅权与复制权，对信息主体与信息处理者之间高度不对称的信息结构加以矫正。《中华人民共和国民法典》（下称《民法典》）第1037 条第 1 款第 1 句明确规定，自然人有权依法向信息处理者查阅或者复制其个人信息；《中华人民共和国个人信息保护法》（下称《个人信息保护法》）第 45 条在此基础上进一步细化了查阅权与复制权的适用规则，一方面确认个人有权向个人信息处理者查阅、复制其个人信息，并规定相

［作者简介］李西泠，湖南师范大学法学院讲师，法学博士。

［基金项目］国家社会科学基金重点项目“人工智能侵权责任研究”（项目批准号：25AFX006）。

〔1〕［英］伯纳德·马尔：《未来技能》，商陆译，中国科学技术出版社 2023 年版，第 61 页。

应的例外情形；另一方面明确个人信息处理者在接到请求后负有“及时提供”的法定义务。相关规定旨在通过赋予个人请求查阅与获取个人信息副本的权利，增强个人对其个人信息处理活动的透明度与可控性。[2] 由于查阅复制权不仅是对《个人信息保护法》第 7 条“公开、透明原则”与个人知情权的具体贯彻，也为个人信息更正、补充、删除等权利的实现提供了制度基础，因而被誉为“个人信息保护领域的大宪章”与“关键性权利”，在个人信息保护法律体系中具有根本地位。[3] 但从实践运行情况来看，查阅权与复制权虽已在规范层面得到确认，但在不同个人信息处理场景中的实际行使却呈现出明显的不均衡状态，面临权利范围界定不清、行使程序不统一、技术限制被泛化等问题。基于此，笔者以个人信息权益中的查阅权与复制权为研究对象，立足不同个人信息处理场景，对查阅权与复制权的适用范围及其行使规则展开系统梳理与规范分析，力图揭示规范确认与实践运行之间的制度落差，并在解释论与制度构造层面为查阅权与复制权的具体适用提供更具操作性的指引。

二、查阅复制权与可携带权的功能定位及适用分工

《个人信息保护法》第 45 条作为构建信息主体访问与控制数据的关键条款，其立法目的与条文结构在学界引发了争议。核心分歧在于该条文究竟是以“可携带权”为中心构建，还是分别规定了查阅权、复制权与可携带权三种权利。笔者认为，尽管第 45 条将查阅权、复制权及可携带权并列规定，但在权利设立的目的、适用场景及法律结构上，这三项权利在功能定位上存在明显差异，对其加以厘清，有助于明确各自的制度意图，防止在实践中出现混用、误用甚至滥用的情形。

（一）三项权利的制度功能区分必要性

有学者主张第 45 条规定的是个人信息可携带权，并从条文的逻辑结构与对比欧盟《一般数据保护条例》（GDPR）第 20 条的角度出发，将该条理解为涵盖获取副本与传输数据两个层次的权利体系，划分为两个权利维度：一是获取信息副本（包括查阅和复制）；二是向其他信息处理者进行数据转移，即信息可携带权的实质体现。[4] 类似观点认为，第 45 条以信息自决为基础，统一规定了个人信息可携带权，包括请求副本和转移数据两个方面。在持该观点的学者看来，该条旨在提升信息主体对其个人信息的控制能力，强调无障碍、直接传输作为制度设计的关键。[5] 然而，也有学者强调该条实质上分段规定了三项彼此独立的权利，即第一项为查阅权，第二项为复制权，第三项为可携带权 [6]，尤其是复制与可携带在传输对象、格式要求、技术路径等方面具有明显差

〔2〕 姜伟、龙卫球主编：《数字法学原理》，人民法院出版社 2023 年版，第 294 页。

〔3〕 许文义：《个人资料保护法论》，台湾三民书局 2001 年版，第 121 页。

〔4〕 李锦华：《我国实践中个人信息可携权的优化进路——基于 66 款 App 隐私政策实证分析》，载《人权》2024 年第 3 期，第 124 页。

〔5〕 杨立新、赵鑫：《信息可携权在个人信息权益中的地位与作用》，载《兰州学刊》2022 年第 9 期，第 98 页。

〔6〕 韩强、吴涛：《个人信息权的内涵、逻辑与体系建构》，载《北京航空航天大学学报（社会科学版）》2022 年第 1 期，第 41 页。

异。[7] 进一步地，从功利主义视角来看，复制权是否应独立存在亦面临实践挑战。在复杂数据场景中，如果信息主体虽取得副本但缺乏足够的技术能力进行处理，且无法进一步传输数据，则复制权的现实意义将受到削弱，其功能价值也会因此被质疑。[8]

虽然在条文解释路径与理论立场上各有焦点，但各观点争议的核心并非在于考察查阅权、复制权与可携带权是否“同源”，而是在于对三项权利是否存在必要区分。若将第 45 条所涉权利一并理解为统一的“个人信息可携带权”，不仅难以解释不同权利在无限制对象、技术条件与程序要求上的显著差异，也容易在实践中模糊各自的适用边界。因此，有必要从制度功能与适用前提的角度进行区分性分析，以明确三项权利各自的规范目标与适用条件。

一是权利设立的制度目的不同。查阅与复制的核心在于保障信息主体的知情能力与决策基础。通过查阅，个人能够掌握其信息被收集和使用的范围；通过复制，个人可以保存、验证或用于自我防护，避免因为非法收集、处理而致其人身财产权益遭受侵害。[9] 相比之下，可携带权不仅服务于个人对其信息的自主控制，还具有更深层次的制度目标，诸如对数据的实体利益价值进行分配 [10]，打破平台垄断、促进数据流动、提升市场竞争活力 [11]，尤其是在平台经济和社交网络高度集中的语境下具备的推动市场结构优化的公共政策功能。

二是涉及的权利关系结构不同。查阅和复制行为本质上是信息主体与个人信息处理者之间的双边交互，处理者作为义务主体须在其掌控范围内履行相应义务。可携带权的实现则是一个多边过程，除了权利人和当前的信息处理者外，还涉及第三方接收者。这意味着可携带权须协调三方之间的技术、法律及合规责任，复杂程度远高于前两者。

三是权利的适用条件存在差异。查阅和复制原则上对所有信息主体开放，只要不构成《个人信息保护法》第 18 条、第 35 条规定的例外情形（如国家安全、他人权益保护等），处理者即应予以配合。可携带权则设置了更高的门槛，其行使需满足国家网信部门规定的前置条件。尤其是对于很多互联网企业而言，数据可能是最重要的资产和优势所在，不同的企业之间存在竞争关系，基本不可能互相提供个人信息。[12]

四是涉及数据类型与处理方式的限定不同。可携带权的适用对象应该为个人主动提供的或履行合同所必需的个人信息，且须满足自动化处理的要求。[13] 这一规定排除了纸质文档或非电子化记录的数据，也未将处理者从第三方收集的数据纳入其中。相对而言，查阅权与复制权的适用范围更为广泛，并不以数据来源或处理方式为限，更侧重于保障数据透明性和个人知情权。

---

〔7〕 龙卫球主编：《中华人民共和国个人信息保护法释义》，中国法制出版社 2021 年版，第 202 页。

〔8〕 杨立新、赵鑫：《信息可携权在个人信息权益中的地位与作用》，载《兰州学刊》2022 年第 9 期，第 107 页。

〔9〕 程啸：《个人信息保护法理解与适用》，中国法制出版社 2021 年版，第 337 页。

〔10〕 王锡锌：《个人信息可携权与数据治理的分配正义》，载《环球法律评论》2021 年第 6 期，第 6 页。

〔11〕 杨合庆主编：《中华人民共和国个人信息保护法释义》，法律出版社 2022 年版，第 115 页。

〔12〕 王利明、程啸、朱虎：《中华人民共和国民法典人格权编释义》，中国法制出版社 2020 年版，第 460 页。

〔13〕 程啸、王苑：《论我国个人信息保护法中的查阅复制权》，载《法律适用》2021 年第 12 期，第 19－20 页。

综上所述，第 45 条的第 1 款、第 2 款和第 3 款虽在结构上紧密排列，但实质上分别承载了不同的制度功能与规范逻辑，将查阅权、复制权和可携带权区分开，既符合立法原意，也有助于在实践中更好地构建权利行使路径与配套保障机制。

（二）查阅权、复制权的基础性地位

从制度功能与适用前提来看，查阅权与复制权并非仅作为可携带权的前置或附属权利而存在，而是在特定个人信息处理场景中具有不可替代的独立适用价值。因为查阅权旨在保障个人对其信息处理状况的知情与核实，是个人行使更正权、删除权、限制处理权乃至提起侵权救济的前提性条件；复制权则通过提供信息副本，使个人能够保存证据、实现外部监督或进行权利救济。尤其是在以信息透明、风险防控与权利核验为核心目标的处理情境中，查阅权与复制权应当属于整个个人信息权利体系运行的前提环节。[14]

例如，在电子商务平台和互联网服务平台中，查阅权与复制权对于保障个人对其交易数据、账户信息及相关记录的知情与核验具有基础性意义。在此类场景下，个人信息的主要功能在于确认交易事实、防范纠纷风险以及应对潜在侵权，而非实现跨平台流转。相较之下，可携带权背后的最终目标是在数字单一市场内提供所有数字服务的互联和互操作性。[15] 因此，通过查阅和获取个人信息副本以实现信息核对与证据留存，更符合该类场景下的制度需求。又如，在涉及个人信息合规审查、纠纷处理或权利救济的情形中，查阅权与复制权具有明显的程序性优先地位。当个人对其信息是否被过度收集、违规利用或错误处理提出异议时，首要需求并非数据流转，而是确认事实、固定证据。在此意义上，查阅权与复制权构成信息主体启动后续救济程序的重要前提，而可携带权则难以承担此类功能。

（三）可携带权的补充性定位

在个人信息权益体系中，可携带权并非对查阅权与复制权的简单延伸，而是一项具有高度技术依赖性与明显政策导向的进阶性权利。对其内涵的理解，通常可区分为两个层次：其一，是信息主体将其个人信息从原有平台“带走”，即摆脱单一信息处理者的事实控制；其二，是在此基础上，将相关数据直接“带到”其他平台，用于账号初始化、历史记录迁移或社交关系延续等用途。然而，上述两层含义并不当然适用于所有个人信息与全部处理场景，立法与实践均对可携带权的适用作出了明显限缩。

首先，从权利体系的结构看，可携带权应被定位为查阅权与复制权之后的补充性制度工具。查阅权解决的是“我有哪些数据在你手里、你如何处理”的问题，复制权则进一步保障信息主体能够取得完整副本，以便保存、核对并行使更正、删除等后续权利。在多数个人信息保护场景中，上述两项权利已足以实现信息透明与个体控制的基本目标。相比之下，可携带权要求信息处理者

〔14〕 徐伟等：《权利的边界：个人信息赋权逻辑及其行使路径》，上海人民出版社 2023 年版，第 20 页。

〔15〕［意］安东尼奥·曼加内利、安东尼奥·尼基塔：《监管数字市场：欧盟路径》，王杰、李炫圻译，上海人民出版社 2023 年版，第 88 页。

按照特定格式对数据进行整理并实现向第三方的传输，其制度成本与技术复杂性显著更高，若将其作为一般性权利普遍适用，反而可能造成权利行使与义务履行之间的结构性失衡。因此，可携带权更适宜作为在特定条件下启动的补充性权利，而非信息主体行使个人信息权利的常态路径。

其次，从适用对象与范围看，可携带权在立法上已被明确限缩。无论是学界共识，还是《个人信息保护法》第 45 条第 3 款及《网络数据安全管理条例》（国务院令第 790 号）第 25 条的具体规定，均表明可携带权并不覆盖所有个人信息。其对象原则上应限于两类数据：一是信息主体主动提供给平台的个人信息，二是为履行合同所必需而收集、处理的个人信息，如电子商务平台中的收货地址、订单记录等。相应地，平台基于自身运营需要形成的用户画像、推荐模型、风险评估结果等数据，不应被纳入可携带权的范围，即区分基础权利行使与衍生需求满足的界限。〔16〕

再次，从行使条件看，可携带权的适用还须同时满足多项实质性与程序性限制。《网络数据安全管理条例》第 25 条对《个人信息保护法》第 45 条第 3 款作出了具体落地安排，强调在权利行使过程中应当重点把握以下边界：其一，身份必须经过严格核验，以防止冒名请求导致个人信息被非法转移；其二，数据范围应当合理，不得以可携带权为名，要求平台提供其商业秘密、算法模型或超出个人信息范畴的数据；其三，技术上应当具备可行性，信息处理者不得仅以实现成本高或系统复杂为由一概拒绝，但亦无义务承担不成比例的改造负担；其四，他人合法权益不得受到损害，尤其是在涉及通讯录、群聊信息或社交关系链等场景中，应防止第三人的个人信息或商业秘密被一并迁徙。

最后，从制度功能看，可携带权的核心价值并不完全在于个体保护，而在于通过促进数据流动、降低用户转换成本，矫正平台锁定效应并改善市场竞争结构。〔17〕正因如此，其适用更适合于平台经济和网络效应显著的场景，而不宜泛化为所有个人信息处理活动中的通行权利。将可携带权限定于特定数据类型、特定处理方式与特定条件之下，既有助于防止其与查阅权、复制权产生功能重叠，也有利于在个人信息保护、数据安全与公平竞争之间实现更为稳健的制度平衡。

综上，通过对查阅权、复制权与可携带权的区分，可以形成如下分析框架：其一，在个人请求了解自身信息处理状况、核实信息真实性或为后续权利救济准备证据时，应优先适用查阅权与复制权；其二，只有在数据具备结构化特征、技术可行且转移目的明确的情形下，方可进入可携带权的适用范围；其三，任何以组织控制结构或技术实现方式为由对查阅复制范围进行限制的主张，均应接受合法性与比例性审查。下文即在此框架下，对不同个人信息处理场景中的查阅复制权行使状况进行具体检视。

〔16〕《北京四中院通报个人信息保护类案件审判情况及典型案例》案例三，https://baijiahao.baidu.com/s?id=1847397802190493436&wfr=spider&for=pc。

〔17〕沈佳燕：《个人信息主体权利行使的民行救济协同论》，载《华东政法大学学报》2025 年第 6 期，第 66 页。

三、不同个人信息处理场景中查阅权与复制权的行使

前文从规范层面对查阅权、复制权与可携带权的制度功能与适用情形作出了区分，可以看出查阅复制权构成了个人信息处理活动中权利保障的基线，而可携带权则是在此基线上的高配应用。然而，权利的规范确认并不当然意味着其在实践中的有效实现。不同类型的信息处理者、不同业务模式与技术架构，均会对查阅权与复制权的具体行使范围与实现方式产生实质影响。以个人信息处理结构的类型化差异为基础，可将分析对象区分为以交易关系为核心的电商平台、以多主体互动为特征的社交平台、以组织控制为基础的企业版软件，以及具有公权力属性的国家机关四种具有代表性的典型场景。

（一）电子商务平台中的查阅复制权

在电子商务平台场景中，个人信息的收集与处理具有高频、持续与高度结构化的特征，平台掌握的信息类型复杂、数量庞大，信息主体对其个人信息的依赖程度亦显著高于一般服务场景。因此，电子商务平台成为检验查阅权与复制权能否有效落地的典型场景。

从规范层面看，《个人信息保护法》第 45 条并未对查阅权、复制权的适用对象作出数据来源或处理方式上的限制。只要相关信息能够识别特定自然人，且不属于法定不予告知的例外情形，原则上均应纳入可查阅、可复制的范围。就电子商务平台而言，至少应当包括以下几类个人信息：其一，信息主体在注册、下单、支付等过程中主动提供的基本身份信息与交易信息，如账号信息、收货地址、联系方式、订单记录、支付记录等；其二，平台在履行合同过程中自动生成的过程性信息，如物流信息、售后记录、退款与纠纷处理记录等；其三，平台基于用户行为持续收集的行为日志类信息，如浏览记录、搜索记录、收藏与评价记录等。

从实践状况看，主流电子商务平台在查阅与复制范围上的开放程度明显偏窄。以淘宝平台为例，其隐私政策显示，用户可以通过登录客户端，依次进入“我的淘宝—设置—隐私—个人信息下载”，在输入接收邮箱地址后，由平台以 Excel 文件形式向该邮箱发送个人信息副本。根据平台实际提供的下载内容，该副本主要包括会员名、绑定手机号、性别、昵称、头像、注册时间、设备名称、设备类型以及最近一次登录时间等信息，整体上限于账户基本信息与设备信息的范畴。然而与上述可下载信息范围形成鲜明对比的是，淘宝在其个人信息采集清单中明确列举了更为广泛的数据类型。其中，基本信息包括在注册淘宝账户、设置个人主页、绑定手机号码、邮箱及支付宝账号等安全信息过程中所采集的个人信息；社交信息则涵盖用户在收发消息、发布动态、点赞或评论等社交互动场景中产生的数据；交易信息则涉及在管理收货地址、收藏夹、购物车及订单履约等过程中形成的各类个人信息。[18] 尽管个人信息采集清单所列信息在形式上“可查阅”，但在“个人信息下载”功能中，并未提供与之相对应的复制内容。平台实际允许下载的数据，仅

〔18〕《淘宝网基本功能隐私政策》，载淘宝网，https://terms.alicdn.com/legal-agreement/terms/suit_bu1_taobao/suit_bu1_taobao201703241622_61002.html?spm=tbpc.pc_sem_alimama/a.1997523009-ft.6.6e2c2a893Xo42X，2026 年 4 月 26 日访问。

限于账户与设备相关的少量信息，而未覆盖其在社交互动、交易履约及行为记录等场景中持续收集并处理的大量个人信息。

由于电子商务平台中的数据既是用户的交易记录，也是平台的商业秘密和核心资产，以技术复杂或商业敏感为由，将大量与个人信息处理直接相关的数据排除在查阅、复制范围之外，往往是出于商业利益考量而进行的有意识限缩，但上述限缩做法难以与查阅权、复制权的制度目的相契合。查阅权并非仅指在界面中零散查看，而是要求信息主体能够整体性地了解其个人信息的处理状况；复制权亦不仅是在形式上提供截图或摘要，而应当允许信息主体取得结构化、可保存的数据副本，以便其核验数据准确性、判断处理合法性，并进一步行使更正、删除等权利。司法实践中，法院已明确指出截图不能准确体现用户个人信息的全部内容，且用户逐页进行截图具有很大的不便利性，信息处理者不能以用户可自行截图为由主张尽到应负的个人信息复制协助或提供义务。〔19〕

（二）社交平台中的查阅复制权

相较于电子商务平台以交易履约为核心的个人信息处理模式，社交平台中的个人信息更具有关系性、互动性与网络化特征。用户在平台上的信息活动不仅涉及自身的身份信息和行为记录，还不可避免地与他人的个人信息交织在一起，如好友关系、聊天内容、互动记录等。

从规范层面看，《个人信息保护法》第 45 条并未因信息的“关系性”而当然排除其适用。只要相关信息能够识别特定信息主体，且不属于法定例外情形，原则上均应纳入可查阅、可复制的范围。那么在社交平台语境下，至少应当包括以下几类个人信息：其一，账户与身份信息，如账号注册信息、绑定的手机号或邮箱、昵称、头像、登录设备与登录记录等；其二，个人内容数据，即由信息主体主动发布或形成的内容，包括文字、图片、音视频、动态、评论及点赞记录等；其三，与个人行为直接相关的互动记录，如好友添加与删除记录、群组加入与退出时间、消息发送与接收时间戳等。

然而，从平台实践看，社交平台对查阅权、复制权的实现普遍采取高度审慎甚至保守的态度。以微信平台为例，其隐私政策对个人信息的收集与使用作出了高度细化的场景化列举，涵盖注册、社交互动、内容消费、位置服务、支付与娱乐等多元业务场景。从信息类型看，微信所收集的个人信息不仅包括用户在注册及个人资料设置过程中主动提供的昵称、头像、手机号码、性别、地区、个性签名等基础身份信息，还包括在产品安全与体验优化过程中自动收集的设备型号、操作系统、设备标识符、登录 IP 地址、操作日志、服务日志及位置信息等技术与行为数据。进一步而言，在朋友圈、公众号、视频号、小程序、群聊、搜索、“看一看”、“听一听”、“问一问”等功能中，平台持续收集并处理大量与用户行为和社交活动直接相关的信息，包括用户发布的文字、图片、视频、评论、点赞记录，内容阅读、播放、搜索、收藏、分享、互动记录，以及基于地理位

〔19〕 北京市第四中级人民法院（2023）京 04 民终 39 号民事判决书。

置、步数信息、音乐与视频偏好形成的使用轨迹数据。[20] 上述信息共同构成了对用户社交关系、兴趣偏好与行为模式的立体刻画，其广度与深度远超单纯的账户信息范畴。

与其高度全面的信息采集实践形成鲜明对比的是，微信目前向用户实际开放复制、导出的个人信息范围极为有限。根据平台提供的个人信息导出功能，用户可获得的数据主要包括昵称、头像、微信号、性别、地区、个性签名、绑定账号（如 QQ 账号）、手机号码，以及登录设备与登录地址等内容，整体上仍停留在账户识别与设备层面的基础信息。但是对于隐私政策中明确列示并持续收集的社交互动数据、内容消费记录、搜索与浏览历史、行为日志乃至部分位置与偏好信息，平台并未在个人信息下载中提供对应的复制内容。

由此可见，在微信这一典型社交平台中，个人信息采集清单所列信息虽然在形式上大多处于“可被告知、可被查阅”的状态，但在复制权的具体实现上，平台却对可导出范围作出了显著限缩。这种做法导致信息主体虽然能够知悉平台在何种业务场景中处理其个人信息，却难以取得与实际处理规模相匹配的数据副本，从而在核验信息完整性、理解平台处理逻辑以及行使更正、删除等后续权利时面临现实障碍。

（三）企业版软件中的查阅复制权

企业版软件兼具个人使用工具与组织管理平台的双重属性，其个人信息处理并非由单一主体完成，而是呈现出平台—企业—员工三方结构。从以钉钉为代表的企业移动办公软件的隐私政策来看，其对个人信息查阅权、复制权的实现采取了以“数据控制权归属”为核心的分层配置模式，并据此对最终用户的权利行使范围作出实质性限缩。

首先，在数据控制权配置上，钉钉明确区分了“个人用户数据”与“企业组织控制数据”。凡是用户以企业成员身份加入组织、使用企业账号开展办公、沟通与协同过程中提交或生成的数据，原则上均被界定为“企业组织控制数据”，其控制权归属于企业组织，而非个人用户本人。该类数据覆盖范围极广，不仅包括职位、部门、考勤打卡、审批记录、日志、文件、群聊信息等日常办公数据，还可能涉及指纹、人脸特征、地理位置、设备日志、行为日志乃至人力资源管理中高度敏感的身份、薪酬、合同状态等信息。钉钉在其中的角色被明确限定为“受托处理者”，仅依照企业管理员的指令处理相关数据。其次，在查阅权与复制权的权利主体安排上，钉钉实际上采取了双轨制设计。对于个人用户自主注册并使用钉钉形成的个人账号信息（如头像、昵称、电话、性别、地区等），用户可以通过客户端路径自行查阅、更正并复制；而对于企业组织控制数据，个人用户并不当然享有直接向平台主张查阅、复制的权利，其查询、更正乃至导出通常须通过企业管理后台，由企业组织或管理员行使相应的数据管理权限。最后，从具体行使路径看，钉钉虽在“您的权利”章节中形式上确认了用户的查阅权与复制权，并提供了“个人信息查询与下载”的操作入口，但该路径所覆盖的内容主要限于个人账号层面的基础资料信息。大量在隐私政策中明确列

〔20〕《微信隐私保护指引》，载微信网，https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy&head=true#1，2026 年 4 月 26 日访问。

示且在办公实践中对个人权益影响更为深远的考勤记录、行为日志、内部沟通内容、人事管理信息等，均被纳入企业组织控制数据范畴，未被纳入个人可直接下载、复制的范围之内。[21]

在乔某与某信息技术有限公司网络服务合同纠纷案中，法院认为根据《某移动办公平台隐私权政策》，员工在企业群内形成的考勤打卡信息，属于“企业控制数据”，其个人信息控制者并非平台，而是用工企业，平台仅系根据企业管理员的选择提供技术处理服务，并不享有独立的处分或披露权限。[22] 可见在企业版移动办公软件的制度设计中，平台往往通过用户协议与隐私政策，将上述个人信息的控制权整体配置给企业用户，从而在事实上削弱了个人作为信息主体对其个人信息的自主支配能力。此种安排导致的结果是，个人虽持续生成并承受相关数据所带来的管理与评价后果，却难以独立行使查阅、复制等基本信息权利，其合理诉求往往被引导至企业内部管理程序，甚至被完全排除在制度视野之外。在移动办公软件使用过程中，用户作为自然人所生成的各类信息，通常均具备可识别特定个人的属性，无论其形成于工作场景还是组织管理情境，原则上均应纳入个人信息的范畴。考勤打卡记录、登录时间、位置信息、操作日志等数据，直接指向特定自然人的身份与行为轨迹，显然满足《个人信息保护法》所要求的可识别性标准，仅因该类信息产生于劳动关系或企业管理框架之中，并不当然改变其个人信息的法律属性。

在《民法典》与《个人信息保护法》已经明确确立个人信息查阅权与复制权的背景下，上述通过隐私政策或用户协议对权利行使设置普遍性障碍的做法，缺乏正当的规范依据。除非符合法律、行政法规规定的例外情形，或者存在妨碍国家机关履行法定职责、损害他人合法权益等法定事由，信息处理者并无正当理由拒绝信息主体行使查阅权、复制权。企业版软件以“企业组织控制数据”为由，对个人信息查阅复制请求作概括性排除，实质上构成对法定权利的不当限缩。进一步而言，对于在用户协议或隐私政策中，通过格式条款方式明确排除或实质限制个人信息查阅权、复制权的情形，法院不宜径行予以认可。相反，应当结合《民法典》关于格式条款的规制规则，支持信息主体主张该类条款构成“提供格式条款一方排除对方主要权利”，从而否定其效力。[23] 唯有如此，方能防止《个人信息保护法》所确立的查阅权与复制权，在组织化、平台化的用工与管理场景中被制度性架空，确保个人信息权益获得实质性保障。

（四）国家机关处理个人信息中的查阅复制权

国家的权力与义务须依托中央和地方各级、各类国家机关予以行使和履行。正是由于国家权

---

〔21〕《钉钉基本功能隐私权政策》，载钉钉网，https://terms.alicdn.com/legal-agreement/terms/suit_bu1_dingtalk/suit_bu1_dingtalk202010070946_49604.html，2026 年 4 月 26 日访问。

〔22〕 杭州互联网法院（2019）浙 0192 民初 8646 号民事判决书。用户上诉后，浙江省杭州市中级人民法院作出的（2020）浙 01 民终 1040 号民事判决中关于用户考勤信息是否构成个人信息，以及信息主体能否基于个人信息权益行使查阅权、复制权等问题，并未作出正面、明确的回应。判决仅指出，用户在二审中已确认其请求平台公司提供考勤信息的目的，在于作为其与原用人单位劳动争议案件中的证据使用；而广东省深圳市中级人民法院已在该劳动争议案件中要求平台提供相应信息。在此情形下，上诉人在本案中提出的诉求，已通过另一诉讼获得支持，故本院不再另行支持。

〔23〕 胡铭、高艳东、陆青、魏立舟主编：《数字法学判例百选》，法律出版社 2024 年版，第 283 页。

力的制度性背书，国家机关在个人信息的获取、使用与提供等方面相较于一般私主体具有显著的优势。在行政管理、公共服务和社会治理高度信息化的背景下，国家机关在履职过程中持续、大规模地收集和处理个人信息，因而常被视为大数据时代最重要亦是最具影响力的个人信息处理者之一。〔24〕《个人信息保护法》在第 35 条中对国家机关处理个人信息的合法性基础与程序要求作出专门规定，明确国家机关在依法履行法定职责范围内处理个人信息时，应当遵循合法、正当、必要原则，并依法履行告知义务。该条规定表明，国家机关在处理个人信息时，并非当然免于个人信息保护规则的约束，而是基于公共目的和行政管理需要以行政主体身份承担相应行政职责的个人信息处理者。〔25〕与私主体处理个人信息不同，国家机关处理个人信息行为性质上属于行政行为，公共利益需要是证成行为合法性与正当性的唯一理由。〔26〕其在履职过程中收集、存储、使用、传输公民个人信息的行为，属于个人信息处理活动，应受第 45 条关于查阅权、复制权的约束。然而在国家机关处理个人信息的情形中，个人信息查阅权与复制权的适用往往与政府信息公开制度产生交叉。

需要明确的是，个人信息查阅权、复制权与政府信息公开申请在权利属性与制度功能上存在根本不同。个人依据《个人信息保护法》行使查阅权、复制权时，其请求对象仅限于行政机关在履行法定职责过程中所处理的、与其本人直接相关的个人信息，权利行使具有明显的个体指向性，其目的在于保障个人对自身信息处理情况的知情、核实。相应地，该类信息的呈现对象仅为信息主体本人，并不发生向社会公众披露的效果，也不以公共利益为正当性基础。具体而言，国家机关处理个人信息的查阅权、复制权，应当主要适用于行政管理与公共服务过程中形成的、以特定个人为对象的个人信息。例如，在户籍管理、社会保障、税务征管、行政处罚、行政许可等场景中，国家机关掌握的大量个人信息，直接关系到信息主体的权利义务状态。对于此类信息，信息主体可依据《个人信息保护法》第 45 条请求查阅和复制，而非通过政府信息公开程序提出申请。〔27〕

政府信息公开制度则具有鲜明的公益属性，其核心在于保障社会公众的知情权〔28〕，以期提高政府工作的透明度，加强人民对政府的监督。〔29〕与个人信息查阅权、复制权不同，政府信息公开的申请主体原则上并不限于信息所涉的自然人，任何公民、法人或者其他组织均有权依法提出申请；一旦相关信息构成依法应当公开的政府信息，其公开效力即指向不特定多数人，而非仅对特

〔24〕张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，载《中国法学》2015 年第 3 期，第 48 页。

〔25〕姚志伟：《大型平台的个人信息“守门人”义务》，载《法律科学（西北政法大学学报）》2023 年第 2 期，第 121 页。

〔26〕杨尚东：《论大数据时代政府信息公开中的敏感个人信息保护》，载《行政法学研究》2025 年第 4 期，第 108 页。

〔27〕例如，纳税人作为个人信息主体，有权向个人信息处理者查阅、复制涉税信息。由于税务部门接收第三方政府部门提供的涉税信息并予以保存，税务部门应作为个人信息主体行使查阅权、复制权的义务主体，查阅、复制的范围即第三方政府部门告知内容所包含的事项。杨同宇：《论政府部门涉税信息共享中的个人信息保护》，载《中国法律评论》2024 年第 5 期，第 221 页。

〔28〕温昱：《个人信息权利体系论纲》，社会科学文献出版社 2024 年版，第 71 页。

〔29〕江必新、郭锋主编：《〈中华人民共和国个人信息保护法〉条文理解与适用》，人民法院出版社 2021 年版，第 419 页；杨伟东：《政府信息公开诉讼研究》，法律出版社 2022 年版，第 198 页。

定申请人发生效力。[30] 因此，当权利人请求查阅的并非与其本人相关的个人信息，而是国家机关在履行行政管理职能过程中制作或者获取的并以一定形式记录、保存的其他信息时，就应当依据《中华人民共和国政府信息公开条例》的规定，向有关行政机关申请信息公开。[31]

四、新技术条件下查阅权与复制权的行使

通过对电子商务平台、社交平台、企业版软件及国家机关等不同处理场景的考察可以发现，查阅权与复制权在实践中的受限也与个人信息处理所依赖的技术条件密切相关。虽前述场景中已存在部分技术应用，但人工智能、自动化决策等新技术正在深刻改变个人信息的处理方式，并对查阅复制权的行使提出新的问题，因此有必要单独探讨。

（一）人工智能处理个人信息中的查阅复制权分层回应

人工智能技术在推荐系统、内容审核、信用评估与辅助诊断等场景中的广泛应用，使个人信息的处理方式呈现出高度复杂化与非线性化特征。当个人信息被嵌入模型训练、特征提取与算法推断之中，信息主体是否仍能够有效查阅和复制其个人信息，成为权利行使的新课题。从技术层面看，无论是利用带有分类标签的实例训练机器学习模型，还是使用不带分类标签数据的算法，都是通过寻找数据中的模式并使用这些模式来作出预测。[32] 在此基础上，人工智能场景中查阅权与复制权的实现，应当在对象与方式上作出合理区分。就查阅权而言，其重点不在于要求信息处理者展示模型内部结构，而在于以明确易懂的语言使信息主体能够了解数据处理活动对个人产生的影响、潜在风险以及数据处理者采取的保护措施等问题。[33] 通过提供数据类别说明、处理目的说明及个人数据使用概览，查阅权仍具有现实可操作性。就复制权而言，其对象应限于可分离的个人信息数据集，如原始输入数据、行为日志、标签结果等，而不应延伸至模型参数、算法规则或由平台投入大量资源形成的模型成果。明确了这一权利边界后，还须进一步认识到权利的存在与否是一方面，而不同场景下权利的行使方式与制度收益则是另一方面。

1. 辅助性应用中查阅复制权的有限意义

以医疗人工智能为例，研究者收集包含肿瘤良恶性诊断结果的患者数据（如年龄、性别、体重等），通过对数据标注“良性”或“恶性”标签，使算法在比对预测输出与真实标签的迭代中不断修正模型，最终能够对新增病例的肿瘤性质作出预测。[34] 在此类应用中，若患者要求查阅复制其个人信息是否被用于训练语料库，首先需要明确权利本身是可以行使的。《个人信息保护法》第45条并未将辅助性场景排除在外，患者作为信息主体，当然有权请求平台告知其个人信息是否被

〔30〕 王锴、周锐恒：《论政府信息公开中依申请公开的对象范围》，载《中南民族大学学报（人文社会科学版）》2022年第8期，第120页。

〔31〕 程啸、王苑：《论我国个人信息保护法中的查阅复制权》，载《法律适用》2021年第12期，第23页。

〔32〕 刘宏等主编：《数据治理概论》，机械工业出版社2024年版，第217页。

〔33〕 叶雄彪：《生成式人工智能背景下的个人信息保护：范式转换与规则完善》，载《法学家》2025年第4期，第70页。

〔34〕 刘宏等主编：《数据治理概论》，机械工业出版社2024年版，第218页。

处理以及处理的具体情况，但该请求的实际制度收益较为有限。虽然在著作权领域，已有法案尝试通过信息披露规则对生成式人工智能的训练数据来源进行规制，如要求生成式人工智能系统的开发者在系统向公众提供之前对训练数据中所包含的受著作权保护的材料进行记录，并标明相应的权利人信息。[35] 此类要求实际上是通过规范模型训练阶段的数据来源，对生成式人工智能可能产生的著作权侵权风险进行“输入端”的前置调控，以防止模型输出内容对著作权人的利益造成损害。相比之下，在医疗类的人工智能应用场景中，模型输出通常仅作为医生诊断决策的辅助工具，并不直接替代医疗判断，也难以对患者个人利益产生类似著作权领域中的输出侵害风险。在此类辅助性应用中，查阅复制权的功能主要体现于知情层面，即让患者了解其信息被处理的事实，但其对于保障核心诊疗权益的纠偏作用相对微弱。

2. 裁判性应用中查阅复制权的核心功能

形成对照的是，在自动化决策等直接作用于个人权益的裁判性应用中（如信用评分、贷款审批、招聘筛选、差别化定价等），查阅复制权具有不可替代的制度价值。在此类场景中，算法系统不再仅仅作为辅助工具，而是直接参与甚至主导对个人作出具有实质影响的判断与选择，其输出结果往往直接关系到个人的交易机会、就业机会乃至财产利益分配。由此，个人信息处理的每一环节均可能对决策结果产生关键性影响，个人信息的真实性与准确性遂成为决策公正性的基础前提。在此语境下，查阅权与复制权的制度功能上升为对自动化决策风险进行前置识别与事后纠偏的核心工具。具体而言，复制权的核心功能在于通过获取与决策直接相关的个人信息副本，使信息主体能够对影响其权益的关键数据进行核验。这些数据通常包括三类：一是信息主体主动提供或在履行合同过程中形成的基础数据，如身份信息、交易记录、履约历史等；二是平台在运行过程中持续收集的行为数据，如浏览、点击、搜索、互动及使用频率记录；三是基于上述数据经算法加工形成的标签、画像或评分结果，如信用分区间、风险等级、消费能力标签等。正是这些数据在算法模型中被反复调用并参与计算，最终对个体产生差异化影响。通过复制上述数据，信息主体得以识别其中是否存在错误、过时或不当关联，如身份信息录入错误、行为数据误判、标签归类失当等。一旦发现此类问题，复制权即与更正权、删除权等形成联动，为信息主体提供实质性的救济路径。[36] 尤其是在高频自动化决策场景中，错误数据往往会被系统持续调用并放大其影响，若缺乏复制权作为证据获取手段，信息主体将难以证明数据存在问题，从而陷入“无法纠错”的困境。

（二）技术限制作为拒绝事由的边界

在个人信息查阅权、复制权及数据可携带权的行使过程中，信息处理者最常援引的抗辩理由之一，便是“技术上不能实现”。该表述看似中性，实则具有高度的不确定性与扩张风险，一方面

〔35〕 California Assembly Bill No. 412 (2025－2026 Reg. Sess.).

〔36〕梅夏英：《社会风险控制抑或个人权益保护——理解个人信息保护法的两个维度》，载《环球法律评论》2022 年第 1 期，第 9－14 页。

以技术复杂性为外衣，容易掩盖信息处理者基于成本、效率或商业利益所作出的选择性不作为；另一方面缺乏明确边界，易被泛化为拒绝履行法定义务的通用理由。因此，有必要在规范层面对所谓“技术上不能”进行类型化区分，并明确其成立条件。

1. 主观不能

所谓主观上不能，是指在现有技术条件下原则上可以实现，但因信息处理者的系统设计、成本投入或运营选择等原因而未能实现。例如，信息处理者以系统架构复杂、数据分散存储、接口尚未开发或实现成本过高为由拒绝提供个人信息副本。在此类情形中，所谓“技术限制”实质上源于信息处理者自身的技术选择或成本考量，而非客观技术障碍。〔37〕《个人信息保护法》所确立的查阅权与复制权，是以信息处理活动高度信息化、数据化为前提而设定的基本权利，其制度预设并不以“零成本履行”为条件。换言之，信息处理者在设计数据处理架构、选择技术路径时，即应将个人信息权利的实现需求纳入系统设计之中，包括数据的可检索性、可导出性以及结构化存储能力等。若信息处理者未作此类预留，而在事后以技术困难为由拒绝履行义务，本质上属于以自身技术选择对抗法定义务的情形，不应获得法律上的正当性评价。

2. 客观不能

与之相对，能够构成正当理由的“技术上不能”，应当严格限定为客观上不能。所谓客观上不能，是指在当前技术条件与系统结构下，相关个人信息确实无法被识别、提取或恢复，且该状态并非由信息处理者规避义务的行为所导致，而是基于技术本身的限制所形成。典型情形包括：其一，因依法删除或已超过法定保存期限而客观不存在，此时履行义务在事实层面已无可能；其二，已被不可逆匿名化处理，原有的可识别性被彻底消除，无法再与特定自然人建立关联。在此类情形中，“不能”并非源于信息处理者主观不愿或管理懈怠，而是基于现有技术条件所形成的客观限制。

五、个人信息查阅权与复制权的完善

现行规范虽已确立查阅权与复制权的基本框架，但在请求受理、身份核验、信息呈现方式及履行标准等方面，仍存在较大的解释与操作空间。为防止查阅复制权在实践中被空置或形式化，有必要从制度层面对其行使规则加以进一步细化与完善，以增强该项权利的可操作性与实质保障效果。

（一）请求受理与身份核验的必要限度

在查阅复制权的请求受理过程中，如何验证请求人身份的真实性是行使机制中的关键环节。

〔37〕例如，在肖某与某科技公司网络侵权责任纠纷案中，法院指出信息处理者以用户缺乏合理的请求理由、实现查阅复制的技术和人力成本过高等为理由，拒绝提供或仅提供部分信息，不符合《民法典》《个人信息保护法》关于个人信息处理公开、透明的原则要求，不属于已完整履行个人信息查阅复制的协助义务。参见《个人信息保护类案件审判情况及典型案例丨北京四中院通报》案例四，https://bj4zy.bjcourt.gov.cn/article/detail/2025/10/id/9044402.shtml。

身份核验不仅涉及信息安全和防泄露风险，更关联到信息处理者的义务边界和信息主体权利的可及性。若身份核验过于宽松，可能导致他人冒名请求查阅复制，产生新的个人信息泄露的问题〔38〕；反之，若核验设置不当、门槛过高，则又可能对信息主体行使权利构成实质性障碍。因此，有必要就身份核验机制的法律正当性、实施限度与技术路径展开进一步分析。

1. 合理性与限度

GDPR 序言第 64 条指出，控制者在数据主体提出访问请求时应采取一切合理措施以确认其身份。《个人信息保护法》第 51 条亦规定，信息处理者应当根据处理目的、处理方式、个人信息种类、对个人权益的影响及潜在的安全风险等，采取相应措施确保处理活动合法合规，并防止未经授权访问和信息泄露。《民法典》第 1038 条、《中华人民共和国网络安全法》第 42 条亦作出类似规定。由此可见，在一般情形下，信息处理者应核验请求发起者是否为请求所涉信息的主体。另外，由于在纷繁复杂的网络空间中，未成年人的心智尚未成熟，对于部分复杂的个人信息处理行为缺乏足够的理解与辨识能力〔39〕，若信息主体为未成年人，则应核验申请人是否为其法定监护人；若信息主体死亡或被宣告死亡，还应核验申请人是否为其近亲属。〔40〕身份核验的正当性不仅在于其保障安全的核心功能，更在于其行使必须恪守必要限度，不得因此损害信息主体的其他合法权益。实践中，部分个人信息处理者以实名认证为由，将信息收集范围从电话号码逐步扩展至姓名、身份证号码，甚至指纹、人脸等生物特征，这种层层加码的做法实质上架空了“最小必要原则”限制处理范围、保障个人信息权益的制度功能。〔41〕为在确保安全的同时落实最小必要原则，身份核验机制可嵌入请求受理环节，通过电子签名等技术手段实现自动化身份认证。〔42〕更为关键的是，信息处理者在完成核验后，不应存储、传输、分析或公开申请人提交的认证材料，而应本着必要限度，在身份验证完成后立即予以删除，从而从源头上避免二次风险。〔43〕

在国际司法实践中，奥地利联邦行政法院（Bundesverwaltungsgericht）就查阅请求中的身份核验标准问题提供了有益借鉴。在一起涉及 GDPR 第 15 条的查阅请求中，数据控制者依据第 12 条第 6 款〔44〕，以对请求人身份存在怀疑为由予以拒绝，法院认为，请求人可以根据具体情况通过多种方式证明身份，包括使用高级电子签名。因此，在请求人使用了《电子识别与信任服务条例》（eIDAS）第 26 条所规定的高级电子签名的情况下，控制者不能仅因此等方式通常不符合受信任

〔38〕 程啸：《个人信息保护法理解与适用》，中国法制出版社 2021 年版，第 349 页。

〔39〕 张素华、尹晓坤：《未成年人个人信息同意能力的理论证成及判定》，载《财经法学》2023 年第 6 期，第 5 页。

〔40〕 郭旨龙：《〈个人信息保护法〉第 50 条（个人信息权利行使保障机制）评注》，载《中国应用法学》2024 年第 4 期，第 186 页。

〔41〕 朱晓峰、林睿尧：《论未成年人个人信息处理中最小必要原则的适用》，载《经贸法律评论》2024 年第 4 期，第 110 页。

〔42〕 Radim Polčák, *Article 12 Transparent Information, Communication and Modalities for the Exercise of he Rights of the Data Subject*, in Christopher Kuner, Lee A. Bygrave, Christopher Docksey eds., The EU General Data Protection Regulation: A Commentary Update of Selected Articles, Oxford University Press, p. 88 (2021).

〔43〕 武长海主编：《数据法学》，法律出版社 2022 年版，第 444 页。

〔44〕 在不违背 GDPR 第 11 条的前提下，控制者在对自然人依据本条例第 15 条到第 21 条所提出的请求持有合理怀疑时，可以请求数据主体提供额外的必要信息来证明身份。

电子身份识别的形式标准，就援引 GDPR 第 12 条第 6 款加以拒绝，除非确实存在关于请求人身份的合理怀疑。此外，奥地利联邦行政法院还指出，控制者若依据第 12 条第 6 款对请求人身份提出怀疑，必须在与请求人的沟通中明确说明产生怀疑的具体理由。〔45〕这一裁判逻辑体现了防滥用与防滥拒的双重平衡理念，值得我国在身份核验机制中借鉴吸收。

2. 技术实现路径

为实现身份核验机制的有效性与合规性，信息处理者在制度设计中应注重技术路径的多元适配性，并确保权利行使的便捷性不被过高技术门槛所阻断。当前较为常见的技术实现路径有以下几类：一是账户登录认证机制，适用于用户已有注册账户场景，通过登录状态或绑定的手机、邮箱进行快速识别，操作便捷，实施成本较低，是多数平台的首选方式。二是多因子认证机制，结合短信验证码、人脸识别、动态令牌等多种方式提高身份核查强度，适用于身份冒用风险较高或信息密度较大的场景，能在一定程度上兼顾安全性与识别力。三是新兴隐私增强技术应用探索，如基于区块链和多因子结合的认证方案，将区块链的去中心化等特性以及采用生物特征的认证模式结合应用于身份认证的场景中。〔46〕

与此同时，为避免身份认证本身成为新的数据收集渠道或安全隐患，信息处理者应严格贯彻《个人信息保护法》的目的原则，即认证过程中收集的身份证明材料、账户信息等应仅限于完成验证所需，并在认证完成后及时删除，禁止另作他用、分析或存储。〔47〕必要时，信息处理者应通过访问控制、加密处理、日志记录等手段提升认证信息的使用安全性。此外，在操作界面层面，信息处理者还应履行明确告知义务，包括身份核验所采集信息的种类、使用目的、保存时限及删除机制等，确保信息主体对自身认证过程享有充分的知情与自主控制权〔48〕，进一步保障其对查阅权与复制权的实质行使。

（二）利益冲突下的协调框架

在查阅权与复制权的行使过程中，个人信息主体的权利请求往往会与平台的数据控制权、商业秘密保护以及他人合法权益发生冲突。对此，不宜简单以任何一方利益为绝对优先，而应在个人信息保护与数据利用之间进行结构化的价值衡量。

第一步，应当明确可查阅复制的信息范围。当前，《个人信息保护法》对于查阅权与复制权所覆盖的“信息范围”并无具体条款列明。这一立法上的留白，使得实践中对于查阅、复制请求所涉信息类型的边界产生较大争议。有观点主张，应将查阅与复制的范围扩展至一切“有助于审查个人信息处理合法性的信息”〔49〕，即不仅包括数据本身，还应涵盖处理规则、逻辑、用途、接收

〔45〕 Bundesverwaltungsgericht, W214 2228346 – 1.

〔46〕 缪文豪、王健翔、郑朝晖：《基于区块链和多因子结合的身份认证方案》，载《计算机仿真》2022 年第 5 期，第 402 页。

〔47〕 周汉华主编、周辉执行主编：《〈个人信息保护法〉条文精解与适用指引》，法律出版社 2022 年版，第 64 页。

〔48〕 常宇豪：《论信息主体的知情同意及其实现》，载《财经法学》2022 年第 3 期，第 86 页。

〔49〕 申卫星：《论个人信息权的构建及其体系化》，载《比较法研究》2021 年第 5 期，第 7 页。

方等所有与数据处理相关的背景信息。亦有观点指出，从权利功能与实践可操作性出发，查阅与复制的范围仍应以《个人信息保护法》第 17 条（信息处理者的告知义务）、第 23 条（处理规则的公开）、第 24 条（重大影响决策的告知）等条款为参照，聚焦于“信息处理活动的必要信息”更为稳妥。〔50〕虽然复制权的原初含义在于“请求信息副本”，而此副本应与查阅时所获得的信息相对应，不存在范围上的差异。〔51〕不过，司法实践与企业操作显示，目前两者的落地状况仍存在不小差异。例如在唯品会案中，法院并未要求信息主体说明请求目的，确认了查阅复制权不依附于特定的目的或利益判断，具有自身的独立性与无动机门槛特征。〔52〕然而，根据前文所述和有关研究对当前市面上主流 App 隐私操作的实证观察，用户在 App 内可查询的信息范围明显大于企业通过复制副本所实际提供的数据类型〔53〕，说明企业在响应复制请求时仍存在压缩或限制信息范围的现实问题。基于此，笔者主张应以实现知情权为核心价值导向，对“可查阅复制的信息范围”作扩大解释。查阅权与复制权的对象不仅应限于狭义上的“个人信息”（如姓名、联系方式、位置信息等），更应包括法定告知义务所涵盖的、与个人信息权益侵害风险息息相关的信息（如何种信息被基于何种目的、由何人在何种范围内、在何时间段内处理等），从而实现个人信息权益防御机制的功能定位。〔54〕只有将数据置于完整的上下文语境中，信息主体才能对数据处理行为作出充分理解与评估，从而有效实现其对个人信息的控制与监督。〔55〕对于个人信息处理情况的了解也是《个人信息保护法》第 44 条所规定的个人对其个人信息的处理享有知情权和决定权的保障。〔56〕具体而言，所有能够识别信息主体身份，或与其存在可识别关联的数据类型，均应属于查阅权、复制权可覆盖的范围。〔57〕原因在于，从法律概念出发，个人信息是指与已识别或可识别的自然人有关

〔50〕许可：《诚信原则：个人信息保护与利用平衡的信任路径》，载《中外法学》2022 年第 5 期，第 1153 页。

〔51〕蔡培如：《个人信息可携带权的规范释义及制度建构》，载《交大法学》2023 年第 2 期，第 62 页。

〔52〕广东省广州市中级人民法院（2022）粤 01 民终 3937 号民事判决书。

〔53〕李锦华：《我国实践中个人信息可携权的优化进路——基于 66 款 App 隐私政策实证分析》，载《人权》2024 年第 3 期，第 130 页。

〔54〕杨芳：《个人信息三元权益论的教义学展开与体系衔接》，载《交大法学》2025 年第 4 期，第 64 页。

〔55〕例如，在对用户进行“画像”的情形下，信息处理者会收集个人大量的碎片化的信息，这些碎片化的信息都属于用户“画像”的组成部分，但是否涉及敏感个人信息的处理，需要结合具体场景来进行判断。参见王利明等编著：《民法典新规则解读与适用 人格权编》，法律出版社 2024 年版，第 647 页。

〔56〕国家法官学院、最高人民法院司法案例研究院编：《中国法院 2024 年度案例 12 人格权纠纷》，中国法制出版社 2024 年版，第 267 页。

〔57〕GDPR 第 15 条的解释实践亦佐证了上述观点。根据欧洲数据保护委员会（EDPB）的权威说明，数据控制者在回应查阅请求时，必须提供“所有与数据主体相关的个人数据”，不得擅自删减、过滤或仅限于控制者主观认定的重要部分。即便某些数据未直接由数据主体提供，或其生成方式复杂，也不应成为拒绝提供的理由。数据主体有权知悉全部涉及其个体的记录，尤其在算法被用于决策或评估时，其输入与输出均构成必要信息。此外，根据 GDPR 第 15 条第 3 款的规定，信息主体有权获得数据副本，控制者须确保其完整性和可理解性。数据应当以结构化、常用、可机器读取的格式提供，必要时附带解释说明，使信息主体能够有效识别处理目的、处理逻辑及处理结果，进而判断是否存在不当使用、歧视性评估等情形。若数据控制者以格式复杂、处理成本高等理由拖延或缩减提供范围，实质上构成对访问权的侵蚀。See *CEF 2024: EDPB Identifies Challenges to the Full Implementation of the Right of Access*, https://www.edpb.europa.eu/ system/files/2025－01/edpb_cef-report－2024_20250116_rightofaccess_en.pdf.

的各种信息，无论其表现形式如何，亦无论其是用户主动提供还是被动产生的。只要相关信息与个人相关，且已被处理者通过收集、存储、加工等方式处理，便已进入“个人信息”的法律范畴，理应成为查阅复制权的客体。另外，从处理目的与用户利益的关联性来看，非主动提供的个人信息同样是处理者用以分析用户习惯、构建用户画像、进行精准推荐的基础素材。这些处理活动直接关乎用户的隐私权益与自主选择，与用户利益紧密相连。〔58〕

第二步，在涉及商业秘密或平台数据控制权的情形下，应当以最小必要原则进行衡量。若信息主体请求查阅或复制的数据能够通过技术手段实现定向提取，而不会暴露算法逻辑、数据结构或其他核心商业信息，则平台不应以商业秘密为由一概拒绝。反之，若相关数据的披露将直接揭示算法模型、数据结构或经营策略，则可以通过限制复制范围、提供概要说明或采用数据脱敏等方式实现权利的替代性满足，以兼顾信息透明与商业利益保护。

第三步，在涉及他人合法权益的情形下，应当重点防止对第三人个人信息或隐私利益造成侵害。〔59〕例如，在社交平台或多主体互动场景中，部分数据天然包含他人信息。在此情况下，可以通过匿名化、去标识化处理或对特定字段进行遮蔽，以确保信息主体能够了解与自身相关的数据内容，同时避免披露他人的个人信息。欧盟法院在案件中亦强调在回应涉及第三方信息的请求时，数据控制者应在查阅权与第三方隐私权之间进行审慎权衡，不得因信息中包含他人数据即一律拒绝提供。若相关信息可通过匿名化或去标识化处理满足请求目的，数据控制者应优先采取此类替代措施，以确保信息主体的查阅权与复制权在最大可能范围内得到实现。〔60〕

通过上述三步协调框架，查阅复制权的行使可以在保障信息主体基本权利的同时，避免对数据创新与信息安全造成不当限制。

（三）“及时提供”的标准

除以上所述，请求处理机制中一个关键的问题是请求的答复期限。虽然《个人信息保护法》第 45 条第 2 款仅以“应当及时提供”的表述规定了处理者的回应义务，但并未明确“及时”的具体期限。

结合相关立法背景与国外经验，合理设定明确的时间界限对于保障权利行使的可预期性与可操作性具有重要意义。GDPR 第 12 条第 3 款规定，数据控制者应在 1 个月内对数据主体的请求作出回应，如情况复杂或请求数量庞大，可将期限延长 2 个月，并须在自收到请求起 1 个月内通知数据主体相关情形和延迟原因。《网络数据安全管理条例（征求意见稿）》曾在第 23 条要求数据处理者对个人信息查阅、复制等申请“不得设置不合理条件”，且“应当在十五个工作日内处理并反

〔58〕 胡怀松：《个人信息查阅复制的条件、范围及个人信息处理者的应对探讨》，载《人民司法》2025 年第 16 期，第 45 页。

〔59〕 例如，在李某某与某科技公司网络侵权责任纠纷案中，李某某作为某科技公司运营的某短视频 App 实名用户，要求该公司以书面形式向其提供其曾观看过的全部视频浏览记录，包含视频名称、创作者账号名称、观看时长或观看完成度、观看时间、视频发布时间、播放量等。法院判决某科技公司向李某某提供一定期间的浏览记录，指出当查阅复制的个人信息和他人个人信息不可分割时，在不侵害其他个人信息主体合法权利的前提下，个人信息处理者可以依法提供。参见《个人信息保护类案件审判情况及典型案例丨北京四中院通报》案例三，https://bj4zy.bjcourt.gov.cn/article/detail/2025/10/id/9044402.shtml.

〔60〕 Case C－28/08 P, European Commission *v.* The Bavarian Lager Co. Ltd., ECLI:EU:C:2010:378.

馈”。[61] 虽然最后出台的《网络数据安全管理条例》删去了该条，用“网络数据处理者应当及时受理”予以替代，但体现了立法趋向。

所谓“及时”，并非意味着信息处理者必须在收到请求的瞬间立即答复，但也不能无限期拖延。实践中，应综合考量多个要素来界定“及时”的边界，包括：请求内容的复杂程度、数据提取与处理所需的时间成本、信息处理者的技术能力与资源状况，以及是否涉及人工干预或第三方调取等因素。[62] 例如，若某用户向社交平台请求查阅近一周的登录记录与聊天时间戳，该类数据往往在平台后台以标准化日志形式保存，技术提取难度较低，应当在数日内完成提供。反之，若请求内容涉及该用户长时间使用行为的深度画像分析，特别是算法对用户行为的评估逻辑，则须跨部门调取并进行适当解释说明，此类响应可适度延长时间，但仍应保持合理性。因此，“及时”的判断标准应体现合理期限内的尽责义务，而非形式主义的绝对时间限度，信息处理者应在确保数据准确性、信息安全与权利实现之间寻求恰当平衡。在实践中，为避免“及时”沦为空洞条款，信息处理者可以主动制定内部处理时限机制，如设定一般请求在 10 至 15 个工作日内完成处理，对于涉及信息跨境流转、历史数据调用或涉及第三方利益的信息，应允许一定的延长期限，同时向信息主体提供延迟的理由说明。同时，如因技术或法律原因无法在合理期限内处理请求，信息处理者仍应在初步接收阶段给予明确反馈，告知其预估的完成时间与潜在障碍，以保障信息主体的知情权和程序参与权。特别是在请求被拒绝或部分拒绝的情形下，信息处理者必须说明拒绝依据，并提供申诉途径或主管机关联系方式，确保权利救济渠道的畅通。

（四）信息可理解性的保障

查阅权与复制权的实现，并不止于形式上的提供信息，更关键的是信息处理者是否以足以使信息主体真正理解的方式完成数据的呈现。若仅提供结构杂乱、术语晦涩或内容碎片化的个人数据，即便技术上满足了提供副本的要求，实质上仍有违查阅复制权赋权知情的立法目的。

随着数据处理技术的高度复杂化，数据主体行权面临技术性消解的困境。有学者曾指出，信息主体要在现实中实现访问权，往往面临层层障碍，如能知道权利的存在、知道如何行使、处理者回应、能理解内容等。[63] 这些不确定性使得查阅复制权在理论上成立，在实践中却难以落实。一名奥地利学生与脸书（Facebook）的交涉清晰揭示了上述问题。尽管脸书提供了 1 200 页的个人信息副本，但信息结构杂乱，未附处理逻辑解释，普通用户难以从中读懂个人信息的处理情况。[64] 即使今日脸书改进了用户信息导出功能，但实践中仍存在导出内容缺失、文件格式混乱、语言晦涩等问题。[65] 有观点曾批评称，若信息处理者继续采用技术性封闭或结构复杂的数据呈现

〔61〕 李婕：《个人信息可携带权的权利属性及实现路径》，载《东北师大学报（哲学社会科学版）》2023 年第 1 期，第 120 页。

〔62〕 程啸：《个人信息保护法理解与适用》，中国法制出版社 2021 年版，第 351 页。

〔63〕 Koops, Bert-Jaap, *The Trouble with European Data Protection Law*, International Data Privacy Law, 250－261 (2014).

〔64〕 *How Much Data Did Facebook Have on One Man? 1,200 Pages of Data in 57 Categories*, Wired (28 December 2012), https://www.wired.com/story/privacy-versus-facebook/.

〔65〕［德］MorBakhoum、BeatrizCondeGallego、Mark OliverMackenrod：《个人数据保护整体性进路 基于竞争法、消费者权益保护法与知识产权法的视角》，文学国、金枫梁等译，上海大学出版社 2023 年版，第 51 页。

形式，“访问权”将沦为“纸老虎”。〔66〕尤其在算法决策逐渐成为日常平台运营常态的背景下，信息主体若无法理解算法背后的逻辑、计算标准和预期后果，其监督能力也无从谈起。有学者因此主张，除了有义务告知数据主体其个人信息被用于画像的事实外，还必须告知其可能产生的预期后果。〔67〕

《个人信息保护法》第 45 条第 2 款虽未明确要求信息处理者解释算法，但若结合第 17 条的告知义务以及第 24 条关于自动化决策的规定，可以推导出信息处理者应负有一定的处理逻辑解释义务。也就是说，在查阅权与复制权的行使中，特别是在涉及用户画像、个性化推荐、信用评分等高风险处理活动时，信息处理者应提供简明、易懂的处理逻辑说明，而不仅是技术性结果。

六、结语

在数据主导的数字社会中，信息处理活动日益复杂，信息主体与信息处理者之间的结构性不对称愈加突出。作为增强数据透明度与实现信息自决的关键制度，查阅权与复制权的有效落实对于个人信息保护体系的运行具有基础性意义。笔者基于《民法典》第 1037 条和《个人信息保护法》第 45 条的条文展开分析，明确其与可携带权的边界，系统梳理查阅权与复制权可覆盖的信息类型与实践机制，强调应以无门槛、可理解与程序保障为核心导向，推动该项权利从形式设立走向实质落实；未来应进一步通过立法解释、监管细化与技术标准制定，为查阅权与复制权的行使提供更为明确、统一与便捷的支持框架，使其真正成为提升信息主体权利实现度与数据治理质量的重要抓手。

The Applicable Boundaries and Exercise Mechanisms of the Right to Access and Copy Personal Information

LI Xiling

Abstract: Although the Civil Code and the Personal Information Protection Law have established the right to access and copy personal information, the exercise of this right varies significantly across different processing scenarios, revealing a notable gap between legal norms and practice. Platform rules, the allocation of data control rights, and technical constraints often narrow its scope of application, thereby undermining its functions of information, control, and

〔66〕 Moerel, E. M. L. & Prins, J. E. J., *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things* (25 May 2016), https://ssrn.com/abstract=2784123.

〔67〕 Hildebrandt M., *The Dawn of a Critical Transparency Right for the Profiling Era*., Digital Enlightenment Yearbook 2012, IOS Press, 2012, p. 41, 51.

oversight. On the basis of distinguishing the institutional functions of the right of access, the right to copy, and the right to data portability, this article clarifies the priority status of the right of access and copying. Through an analysis of typical scenarios—e-commerce platforms, social media platforms, enterprise software, and public authorities—it reveals the primary limitations on the exercise of this right. In response to obstacles arising under new technological conditions, it proposes strict scrutiny of the legitimacy of "technical limitations" and recommends improving the exercise rules in terms of request handling, timely provision, and information intelligibility, so as to promote the substantive realization of the right of access and copying.

Keywords: Personal Information Protection; Right to Access; Right to Copy; Informational Self-determination; Contextual Application

（责任编辑：王乐兵　汪友年）