信息≠数据：一个双向结构性问题

——兼与混同论商榷

商建刚

【内容摘要】当前学界对于信息和数据的关系仍存在较大争议。混同论这一代表性观点认为个人信息与个人数据本质上具有一致性，但这种观点未能有效评估信息和数据在法益基础、权利属性及制度功能方面的差异，进而导致信息被误认作数据而遭到滥用，同时数据被误认作信息而引发数据垄断等问题。这种双向的结构性问题提示我们，对个人数据与个人信息应当明确区分。目前学界关于区分论的探讨大多集中于“为何需要区分”的问题，尚未构建起一个系统的“如何进行区分”的理论框架。数据作为一种新型的生产要素，其价值应被理解为大数据所特有的“计算价值”，这一价值与传统意义上信息的“识别价值”存在显著差异。基于此理论，通过“事实、认识、功能”的综合判断路径，可以在制度层面实现对两者的明确区分。具体而言，应在事实层面，厘清本体差异；在认识层面，区分适用目的；在功能层面，明确制度差异。对数据与信息的区分，不仅有助于应对实践中数据利用与信息保护之间的矛盾，也可以为构建符合我国国情的数据治理体系提供更为精细且可行的理论支持。

【关 键 词】个人数据流通　个人信息保护　生产要素理论　数据计算价值　信息识别价值

【作　　者】商建刚，上海政法学院经济法学院副教授。（上海 201701）

【基金项目】研究阐释党的二十大精神国家社会科学基金重大项目“加强重点领域、新兴领域、涉外领域立法研究”（23ZDA075）；上海政法学院 2025 年校级一般项目“知识蒸馏‘软标签’的法律定性研究”（2025XYB04）

关于个人数据与个人信息关系的争论

在有关数据的复杂研究中，数据与信息之间的关系曾长期处于模糊不清的状态。进入数字社

会以来，面对个人信息保护的现实需求和大数据蕴含的巨大商业潜力，学界开始涌现出将个人信息与数据资产明确区分的声音。[①]2017—2021 年,《网络安全法》《数据安全法》《个人信息保护法》这三部关键法律相继施行。然而，它们均未明确界定信息或数据的法律内涵，且不同法律对数据和信息所给出的定义存在差异。[②]在此期间，已经有学者认识到，信息 / 数据具有人格权和财产权的双重属性，且数据和信息在计算机处理过程中位于不同的结构层级，在个人信息保护中也同样需要尊重数据的流通价值。然而，该问题在当时并未引起广泛讨论。

2021—2023 年，数据与信息的法律区分开始引起学界的广泛关注。既有研究已基本解答了两者“为何要进行区分”的疑问，[③]但“如何建构”与“如何适用”的问题一直悬而未决。其主要原因在于：首先，理论研究已阶段性完成，主要集中于对必要性的论证；其次，立法与司法层面对数据与信息权利结构的回应尚不明确；再次，生成式人工智能、数据跨境流通、数据资产化等现实议题的兴起，导致数据法的研究重心逐渐转向更为紧迫的技术治理与制度适配问题，从而使数据与信息的区分问题逐渐被边缘化。我们已经步入一个“信息不再足以全面代表数据”的时代，面对生成式 AI、数据要素市场、数据跨境流通等全新挑战，重新探讨并确立“数据”与“信息”在法学中的独立地位，不仅势在必行，更是重塑数据权利体系、回应实践需求的紧迫任务。

目前，关于“个人信息”与“个人数据”关系的议题，学界主要形成了区分与混同两种截然不同的立场,分别反映对于数据治理目标、法益配置逻辑以及制度功能的不同理解。“混同论”认为,“数据”与“信息”在本质上属于同一概念范畴，二者仅在表述形式上有所区别。个人数据权利在法律本质上是对个人信息权益的具体化体现。[④]从价值实现的维度来看，信息的交换价值必须依托于数据载体才能得以显现，而数据的存在意义则取决于其承载的具体信息内容。据此认为，数据是信息的“高级形态”，不仅包含基础信息内容，还通过数字化处理赋予了信息可计算、可处理的新型价值形态。个人数据中具有经济价值的部分，正是通过数据形式固化的个人信息。个人数据与个人信息本质上指向同一客体。数据作为信息的唯一数字化表现形式，脱离信息的“纯数据”或缺乏载体支持的“信息”都不具备实际规范意义。[⑤]因此，“混同论”主张没有必要刻意区分个人数据与个人信息。适用于个人信息保护与利用的法律规则，自然也应适用于个人数据处理活动。[⑥]

本文否定将“数据”与“信息”混同的做法，因为其忽视了两者在生成路径、认知结构和法律属性上的根本差异，也容易导致法律规制范围的模糊和制度功能的错位。首先，从认知结构来看，信息是数据经过筛选、加工和解释后的结果，具有明确的语义内涵和主观参与性；数据则是对客观事物状态的原始记录，具备非表达性和非语义性，二者在认知层级上并不对等。其次，从法律属性来看，信息可以纳入现有的知识产权或人格权保护体系；而数据则更具资源性、工具性和可再利用性，亟须以“生产要素”的视角构建独立的权利框架。再次，若不区分数据与信息，极易将数据的经济价值误归于信息的经济价值，导致数据要素化及数字经济中所需的产权确权、资源配置等制度基础缺乏。因此，在法律规制上，有必要承认数据是独立客体，并以差异化制度回应其与信息在功能和治理目标上的不同。

显然，区分二者并非简单的概念游戏，而是解决法益错位、规则偏差和治理失衡问题的关键。“区分论”强调应将“数据”与“信息”进行明确而严格的甄别。第一，数据与信息的本质不同。从哲学角度来看，信息属于内容范畴，而数据是其形式化的载体，二者的关系类似于著作权法中的“作品”与“载体”。换言之，信息侧重于“内容”，而数据侧重于“表现形式”；信息可被理解为“关于客体的知识”，而数据是“信息的形式化呈现”。[⑦]第二，根据当事人利益的侧重点、

诉求的性质以及救济方式的不同，涉及数据与信息的法律问题在实践中已经被区分为信息问题和数据问题。[8]实践表明，信息更侧重于人格利益，属于受人格权保护的人身权益；而数据则更强调财产属性，属于受财产权保护的财产权益。第三，在制度功能层面，法律及司法文本中对“数据”的内涵界定模糊，往往与“信息”一词交替使用，缺乏明确的区分，[9]而进行区分有助于完善司法保护举措。

因此，本文在现有研究基础上，进一步剖析两者的差异及治理逻辑。尤需追问的是，个人数据与个人信息应如何区分？区分后如何与现行制度有效衔接？本文试图从“数据计算价值”与“信息识别价值”的新视角，提出“个人数据”与“个人信息”的区分理论，旨在为将数据作为一种新型生产力的数据治理体系提供更具解释力与实践指导意义的理论支撑。

个人信息与个人数据的本质差异

如上所述，“混同论”忽视了个人信息与数据的差异性，导致二者权利边界模糊，这不仅阻碍了数据要素的市场化进程，也无法有效保障个体权益。从实践角度出发，个人信息与个人数据在法益保护基础、权利属性结构，以及制度功能定位方面存在本质区别。

（一）二者所保护的法益基础不同

当前的法律体系将个人信息视为隐私的延伸，这使得个人信息保护规则几乎成为隐私权在数字时代的翻版。《民法典》第 1034 条设立了“私密信息”的概念，而《个人信息保护法》第 28 条则界定了“敏感个人信息”的定义，两者之间存在交叉与重合。换言之，若某项信息同时满足敏感个人信息和私密信息的判定标准，那么它符合个人信息保护与隐私保护的双重标准。[10]然而，隐私是一个与个人自主权紧密相连的概念，其重要性在于明确划分公共领域与私人生活之间的界限。隐私权是指在社会群体生活中，个体享有免受打扰的权利。在当下的信息保护制度中，以“识别”与“可识别性”作为核心标准，将所有能够识别特定个人的信息纳入保护范畴，并通过限制收集、使用和传播等手段，有效维护个人的自主权，实质上是对隐私保护逻辑的延伸。

如今，个人信息的范畴已显著扩展，隐私保护的路径也从信息保护领域拓展至数据保护领域。可以说，“个人信息的概念经历了一个由窄至宽的发展演变过程”。[11]从最初仅保护姓名、身份证号、住址等可直接识别个人的信息，逐步扩展至涵盖网络标识、消费记录等所有能够间接识别个人的数据。在未明确区分“数据”和“信息”的情况下，数据保护规则被视为信息保护规则的延伸。由此产生了传导效应，隐私保护的法律范式不仅覆盖了个人信息领域，还扩展至数据领域。然而，隐私和数据分别承载着不同的价值逻辑，二者之间存在内在张力。数据的价值在于流通、共享和利用；而隐私的价值则在于划定个人生活的边界，使主体在社会交往中能够维持不被干扰和窥探的空间。基于隐私权逻辑形成的信息保护规则，不宜直接应用于数据治理领域。

一个显著的例证是，《个人信息保护法》第 50 条引入了个人信息保护的行权机制及私人诉权。由于该机制未能有效区分个人数据与个人信息，导致权利行使的对象涵盖所有与个人相关的数据和信息，从而引发了一系列问题：个人信息主体的行权客体究竟是什么？例如，当个人行使可携带权时，携带的究竟是个人数据还是个人信息？未来，如果个人信息或个人数据已被人工智能学习，个人在行使“被遗忘权”时，需要被遗忘的究竟是个人信息还是个人数据？基于数据的流通价值功能，个人携带权的标的应该是信息而非数据，“被遗忘权”的标的应该是个人信息而

非数据。因为数据的价值在于流通、共享和利用，若允许个人随意携带或删除数据，将极大阻碍数据的流通和价值的实现。个人信息作为隐私权的客体，其保护的重点在于防止未经授权的访问、使用和披露，以维护个人的生活安宁和自主决定权。因此，当个人信息被非法收集、使用或泄露时，个人有权要求删除或更正这些信息，以恢复其生活的私密性。据此，信息应该成为“被遗忘权”的标的。而个人数据作为数字经济的核心生产要素，其价值在于通过分析和利用这些数据来优化决策、提高效率和创新力。可携带权的标的应是个人信息而非个人数据。

个人信息关乎人格尊严等个体法益，而个人数据则涉及流通利用等社会法益。两者的价值取向与保护逻辑在本质上存在差异，对其进行混同处理将直接引发制度目标的冲突。

（二）二者的权利属性结构不同

当前，数据治理领域的理论路径呈现出多元化趋势，讨论焦点集中在是否赋权上。“赋权论者”力图通过知识产权、数据库权、人格权、新型财产权、隐私权等多种权利体系，构建数据主体的权利基础；“非赋权论者”则从合同法、竞争法、控制权理论等视角出发，强调制度设计的灵活性与功能性。尽管现有研究各有其逻辑起点和制度构想，但至今尚未形成统一、系统的数据赋权理论。其根本症结在于，学界和立法实践始终未能明确区分“个人数据”与“个人信息”，导致理论构建的对象模糊不清，进而使赋权依据、权利边界与治理逻辑难以清晰确立。换言之，理论多元化的表象背后，隐藏着客体范畴不清所带来的基础性困境。以“知情同意”这一个人信息保护的基本原则为例，在个人数据与个人信息混淆的情况下，既无法有效保护信息主体的权利，也难以合理规范数据利用行为，进而在技术与资本扩张中催生一系列“伪保护”与“真垄断”的治理难题。

根据我国现行法律规定，在个人信息收集环节，企业等相关主体必须充分获取用户的同意，方能规避后续处理行为的违法风险。然而，在实际操作中，企业通常会制定繁复的隐私政策，普通公众难以准确把握其具体含义；用户对隐私政策的同意，未必真实反映其意愿，可能仅是出于获取服务的无奈之举。[12]这就导致企业与用户之间形成了一种双向的“形式同意”，进而使知情同意原则的功能面临实质性失效。此外，知情同意原则的失效也使得“最小必要原则”难以有效落实。尽管以互联网企业为代表的行业已经针对“最小必要原则”制定了一些场景化的规定，但这些规定本质上仍属于管理性规范，企业依然可以通过“伪同意”的方式予以规避。[13]

同时，由于个人信息与个人数据之间的界限模糊不清，实践中常常出现以保护个人信息为名，实则进行个人数据垄断的现象。数据产业正从以生产为导向的“数据资本化”阶段，向通过数据实现再生产的“资本数据化”阶段过渡。个人数据流通垄断的根源并非个人数据的稀缺性，而是资本扩张过程中对数据控制权的持续强化。[14]正如学界持续批判的“微博诉脉脉案”所确立的数据流通规则，数据共享必须严格遵循“用户授权 + 平台授权 + 用户授权”的三重授权原则。数据控制者可能会以“保护个人信息”为由，拒绝向竞争对手或公共平台开放数据，[15]从而实现数据垄断。

显然，当前实践正面临着信息失控与数据垄断并存的困境，而其根源就在于现有研究尚未突破“混同论”的思维局限，不加区分地将数据和信息作为单一主体“所有”或多主体“共有”的客体，忽略了二者在价值取向上的差异。简言之，个人信息更接近于人格权或支配权，而个人数据则更具共享性、关系性和相对性。这种混同处理导致理论对象模糊、治理逻辑混乱，在实践中表现为知情同意机制失灵、假保护真垄断等现象频发。

（三）二者的制度功能定位不同

个人信息保护与数据治理在制度功能上分别服务于两种不同的目标。个人信息保护重在限制和防御，旨在保障个体隐私和自主权不受侵害；而数据治理则侧重于配置和流通，强调数据作为生产要素在经济与治理中的高效利用。基于各自不同的制度功能，二者在规则设计上呈现出截然不同的逻辑思路。个人信息保护强调个体对信息的自主控制权；数据治理则通过识别安全性并进行分类分级，以防范数据的公共风险。例如在数据领域，《数据安全法》将数据区分为“个人信息”和“重要数据”两大类别，而《网络安全标准实践指南——网络数据分类分级指引》则将数据细分为一般数据、重要数据和核心数据三个层级。[16]在信息领域，个人信息泄露可能引发个人风险，《个人信息保护法》将个人信息区分为一般信息与敏感信息，重点保障信息主体的个体权益。个人信息保护与数据治理的功能分化，本质是数字时代“权利本位”与“发展本位”的辩证统一。然而，面对跨领域、跨行业的数据流通需求，这些分类标准在实际操作中却难以有效对接。

这种张力在匿名化处理机制上尤为突出。作为一项旨在平衡个人隐私与数据利用的技术工具，匿名化制度在实践中因标准宽泛、操作模糊而陷入困境。其结果是，信息处理者因法律要求严格、难以判断是否达标而面临合规焦虑，监管机构则担忧匿名化可能成为数据滥用的技术掩护，用户普遍质疑其隐私权益是否得到切实保障。在此背景下，匿名化机制反而陷入失效的僵局。进一步来看，匿名化制度失效的根源在于数据与信息管理制度之间的功能差异。实际上，匿名化的本质并非绝对安全，而是强调风险的可控性。在人工智能与数据挖掘技术高度发达的背景下，即使数据完成了匿名处理，仍有可能通过“去匿名化”手段重新被识别。在这种情况下，如果制度仍将“不可识别性”作为合法使用数据的唯一前提，反而会导致数据处理者承担超出其控制范围的法律责任。[17]匿名化机制暴露了制度功能差异所引发的困境，而在更广泛的数据治理实践中，类似问题亦屡见不鲜。实践中，既要警惕数据处理对个人隐私权的潜在侵犯，又要兼顾数据流通对公共安全保障和产业发展的积极推动作用，这使得数据处理者和监管机关均承受着巨大压力。因此，应在法律概念上明确区分“数据”与“信息”，并依据各自的制度功能实施差异化治理。

总之，在现行法律框架下，由于未能准确区分“数据”与“信息”，不同制度功能之间的冲突日益凸显，治理逻辑也常常陷入两难境地。值得注意的是，尽管数据与信息在法益基础、权利属性和制度目标上存在本质差异，但在实际操作中，二者往往紧密相连、难以截然分割。如果只是一味强调二者的差异，无法提出清晰、可操作的界分标准，反而可能导致制度空转，仅停留在理论争论层面。因此，更为关键的问题在于如何建立科学合理的区分标准。

数据的计算价值：一种被忽视的效用维度

随着数据挖掘、机器学习等技术的迅猛发展，人们已深刻认识到，数据本身蕴含着超越单纯信息层面的价值。然而，这种价值往往被视作“理所当然”，长期以来被视为数据使用的“自然属性”，在司法实践中仅被反垄断法纳入“竞争性权益”的范畴，这显然难以实现对数据创新成果的全面保护。例如，“行为痕迹”作为个体在数字环境中生成的动态记录，虽然在原始状态下呈现碎片化趋势且价值较低，但经过算法的精准计算后，能够揭示群体行为规律，从而支撑市场主体预测、决策与创新。实际上，数据区别于信息的核心价值在于其通过计算过程所释放出的增值能力。为此，有必要进一步回归数据本身，深入探讨其作为新型生产要素所独有的“计算价值”。

（一）数据计算价值的基础理论：生产要素的功能转换

在小数据时代，数据与信息的区分主要依赖将数据置于特定的语义语境中进行识别。尽管数据与信息在物理层面上紧密相连，但在法律概念上却存在明确的界限。数据本质上是一种未经处理、未被赋予语义的原始符号，属于中立且无意义的“原材料”。只有经过加工处理，并嵌入语境和语义框架中，数据才能转化为具有可读性和可用性的“信息”。从信息论的视角来看，数据是系统的输入，而信息则是通过处理过程排除不确定性后的输出。换言之，信息的意义在于其能够在特定语境中被理解，并传达出排他性的陈述；而数据唯有与语境、语义或特定应用场景相结合，方能显现其信息价值。[18]例如，孤立的“25”仅仅是一个数据，而一旦被解释为“25℃”，便转化为具有实际意义的信息。这揭示出，信息与数据的区别并非基于其物理形态的不同，而取决于其嵌入的解释框架及所服务的应用目的。

此外，数据与信息之间存在着明显的可区分性，混同论实际上是用技术工具性掩盖了法律的价值理性。如前所述，现有数据治理制度的理论基础源自美国的公平信息实践原则（FIPs），其核心概念基于隐私保护。 而在当今的大数据时代，数据的内涵早已超越了传统的隐私价值或信息识别价值，但全球范围内各国数据治理的基本逻辑仍然以保护隐私和信息为核心，导致数据的计算价值未得到充分重视。

随着数字技术的不断进步，数据的属性和作用得到进一步拓展，突破了小数据时代仅基于语境和语义的区分逻辑。生产要素理论为我们提供了一个更为精准的分析框架：任何具备可投入性、配置性以及产出转化能力的资源，均可被视为生产力的核心要素。自萨伊时代起，土地、劳动与资本始终是经济活动中的三大基石。随着现代经济学的演进，技术作为核心生产力被纳入其中。如今，伴随数字技术的迅猛发展，数据凭借其可采集、可配置、可流通以及可转化为有价值成果的独特属性，已然被确立为第五大生产要素。数据作为新型生产要素，正快速融入生产、分配、流通、消费和社会服务管理等各环节，发挥“乘数效应”成为推动经济社会高质量发展的重要动力。从生产要素的视角来看，数据的核心价值在于其通过计算过程所释放的增值能力，本文将其称为“数据计算价值”。经过算法、人工智能或建模分析，数据能够转化为企业洞察、行为预测、决策优化等新产出，从而提升生产效率和社会资源配置能力。相较之下，传统的“信息识别价值”主要体现在数据与自然人身份的关联性上，属于人格权保护的范畴。因此，从生产要素的角度出发，数据的核心价值不在于“其所是”，而在于“其所能”。

（二）“事实、认知、功能”层面的综合区分标准

当前制度对个人信息与个人数据的规定，实际上采用了两种不同的标准：个人信息治理以隐私权为基础，采用识别标准；而个人数据治理则以数据安全为基础，采用计算标准。从本质上讲，现有的区分逻辑类似于一种“静态”逻辑，即一旦将某数据或信息认定为个人数据或个人信息，无论其处于何种场景，都需依据相应的标准进行治理。这种治理模式的弊端在于，无法适应数据或信息的“动态”转化特性，一旦完成分类，便难以实现其他价值。

区分个人数据与个人信息的关键，在于明确“数据计算价值”与“信息识别价值”的差异。这种区分并非简单地将“数据视为数据，信息视为信息”，而是需要采用一种动态的分析范式。数据与信息通常处于一种兼具识别价值与计算价值的二元叠加状态，类似于物理学中的“波粒二象性”。只有在特定的应用场景（“观测空间”）中，才需根据实际用途进行区分。在计算场景下，个人数据和个人信息仅利用其计算价值，均可被视为“个人数据”，此时无需遵循现有法律中关于个人信息

的治理标准；而在识别场景下，个人数据和个人信息仅利用其识别价值，均可被视为“个人信息”，此时需要严格采用现有法律中的个人信息治理标准。结合个人数据和个人信息在信息论视角下的关联性，以及在法律视角下的价值区分性，我们可以构建出区分两者的清晰理论路径。

1. 事实层面：人类可读性与机器可读性的判断

区分的第一步，是对数据的物理形式和表达载体进行客观区分。从事实角度来看，个人信息具有人类可读性，而个人数据则具备机器可读性。就个人信息而言，它以人类能够理解并处理的形式存在，如文本、图像或声音等，无需经过转换或解析即可直接明确其含义。与之相对，个人数据通常以机器可读的格式存储和处理，必须借助计算机程序解析才能被人类所理解。这种机器可读性在域外立法中也有所体现。欧盟《通用数据保护条例》（GDPR）第 20 条指出，数据可携权要求数据以“结构化的、常用的、机器可读的格式”提供，体现了数据的机器可读性视角。根据美国国家标准与技术研究院的定义，机器可读数据指的是“能够被信息系统自动识别和处理的数据格式”。[19]由此可见，个人信息与个人数据在识别价值和计算价值上的差异，从其存在形式上便已奠定了基础。因此，区分的首要步骤在于判断数据是否以人类可直接理解的“信息”形式呈现，还是需要通过程序解析的“数据”形式存在，以此作为后续治理规则选择的基础。需要提醒的是，此层面的判断侧重于对客观事实的识别与确认，要避免过早引入价值判断。

2. 认知层面：主观性与客观性的辨识

在事实判断之后，还需从认知层面进行更深入的区分。从认知角度分析，个人信息具有主观性，而个人数据则展现出客观性。个人信息往往与特定语境紧密相连，其识别价值取决于个体的主观感知。例如，姓名对公众人物与普通人的影响显然存在差异。相较之下，个人数据以符号形式在算法逻辑中运行，其计算价值主要依据客观标准，不受主体差异的影响。[20]此层面的判断，重点在于信息对个体权益的影响程度。通过分析信息的使用是否涉及对自然人身份的识别，以及是否可能引发隐私或人格权的侵害风险，来判定该信息是否应作为个人信息受到更严格的保护。相反，若信息主要用于不依赖身份识别的计算与分析，其认知价值相对客观，此时可将其纳入个人数据治理的范畴。

3. 功能层面：人格权益价值与生产要素价值的评估

区分的最后一步，是结合处理的法律目标和治理功能进行区分。从功能角度来看，个人信息关乎人格权益，个人数据则属于生产要素。有观点可能会认为，个人数据同样需要保护其承载的人格权益，个人信息也具备生产要素属性，这实际上正是两者混淆的关键所在。在某些情况下，企业收集个人信息或通过第三方获取数据，其真实意图并非精确识别特定个人，而是为了进行数据挖掘从而获取个人数据。[21]具体而言，当信息的主要功能在于保护个体隐私权利、维系人格尊严时，应优先遵循人格权保护逻辑，设定严格的流通限制；而当信息作为经济资源或创新驱动力时，则应采纳数据财产权与合规治理框架，以促进其合理利用。

理论区分视角下个人信息保护实践的新阐释

通过明确区分“数据计算价值”与“信息识别价值”，我们可以构建个人信息与个人数据的“区分理论”。基于这一视角，我们能够重新审视相关实践中的困境，并对个人信息保护的核心制度进行更为深入的阐释。

（一）“区分理论”视角下对知情同意原则的再审视

面对获取同意的难度加大、同意成本攀升、同意能力欠缺、同意效果虚化或异化等现实困境，部分学者对知情同意原则作为事先同意规则的实际效用提出质疑，并倡导建立以事后审查为基石的合理适用标准，并且在此基础上提出了多种可行性方案。无论这些观点的具体主张如何，知情同意原则不再适应大数据时代的需求似乎已成为普遍共识。

不可否认，当数据处理的目的在于识别个人身份时，知情同意原则显得必要且有效。然而，在构建大数据模型的场景中，个人信息处理者所追求的并非识别个人身份，而是挖掘个人数据的计算价值。依据区分理论，知情同意原则应限定在实现“信息识别价值”的情境中适用。部分学者指出，知情同意原则在个人数据流通中的核心作用在于消除个人数据处理的非法性。[22]随着技术发展，个人数据的处理方式和目的日益多样化，知情同意原则的全面适用显得力不从心。在大量非识别性个人数据的处理场景中，要求事先获得个体的知情同意不仅效率低下，还可能阻碍数据的合理流动与利用。因此，区分理论提供了一种更为精细的视角，主张仅在涉及能够识别或复原个体身份的个人信息处理时，才应严格适用知情同意原则。对于在收集环节已经过匿名化处理或去标识化处理，或者收集后无法直接识别个体的数据，可以采取更为灵活的处理规则，以促进数据的创新与利用。域外实践表明，在全社会普遍采取充分个人信息保护措施的前提下，个人数据的流通不会对个人信息保护产生负面影响。

而在司法实践中，尚未对信息识别价值与数据的计算价值进行明确区分，这导致司法裁判与社会认知之间的脱节。尽管法院在“微信读书案”与“抖音案”中引入“合理隐私期待”与“场景化识别”等概念，试图区分不同情境下的数据处理方式，但仍依赖“可识别性”这一标准，将数据纳入个人信息保护体系。微信好友列表、社交关系等信息虽具备识别性，但在算法推荐、行为分析等应用场景中，主要发挥计算性作用。其核心价值并非指向身份，而是数据本身所蕴含的计算价值。然而，法院并未对这两种不同的价值属性进行实质区分，而是将所有可识别数据一概纳入知情同意义务的范畴。这种泛化的适用方式忽视了数据计算价值的独立性，弱化了数据要素在社会生产中的功能性定位。

综上所述，知情同意原则作为个人信息保护的核心制度，在大数据和个人数据广泛流通的背景下，正面临适用范围与功能效果的双重挑战。基于“区分理论”的视角，应明确知情同意原则主要适用于保护个人信息识别价值的场景，而非对所有个人数据处理均要求同意。未来的制度设计应推动知情同意原则与数据流通机制的差异化规范，旨在实现信息安全保护与数据合理利用的双重目标。

（二）“区分理论”对可携带权的阐释：专注于个人信息而非个人数据

我国《个人信息保护法》在规范个人信息保护的同时，也涵盖了许多与个人数据流通相关的规则，其中最具代表性的便是对“个人信息可携带权”的规定。从法理角度来看，个人信息可携带权源于个人信息的人格权属性，其核心功能在于通过保障个人的尊严和自主性，赋予个人对其个人信息一定程度的控制权。然而，个人信息可携带权的实施在个人与企业之间引发了诸多挑战。一方面，互联网平台可能通过付费访问限制或技术壁垒，阻碍个人信息的有效转移；另一方面，跨平台数据流通可能加剧“马太效应”，导致数据向大型平台集中，进一步强化垄断，背离竞争法精神。[23]

这一问题的核心在于未明确可携带权的“携带对象”，即个人可携带的究竟是个人信息还是个人数据。个人信息作为人格权的一部分，自始至终由个人完全享有，可以进行携带或根据个人

意志进行迁移属于“我的”信息；相比之下，个人数据的生成依赖数据持有者的处理行为，属于“关于我的”数据，信息主体并非绝对控制者。数据持有者基于其加工、整合等处理行为，对个人数据享有有限的开发使用权利。因此，个人信息可携带权的实施实质上是一种处分行为，既应保障个人信息主体的控制权，也不能损害数据持有者依法享有的有限权利。

基于此，享有可携带权的“携带对象”应限定为未经加工的纯粹个人信息，而非经过加工、整合形成的个人数据。换言之，个人在行使可携带权时，应仅拥有对原始、未经处理的个人信息的转移权利。数据处理者无需将其开发形成的个人数据一并转移，以此实现对人格权的保护与数据经济合理发展的平衡。

（三）“区分理论”对删除权的界定：删除个人信息而非个人数据

在数字时代，个人的网络活动痕迹会被全面记录，并且理论上可以永久保存。这使得“遗忘”这一社会生活更新的重要条件实际上已不复存在。目前，《个人信息保护法》第 47 条的核心要义在于，除了在个人信息收集目的已实现或个人信息处理者存在违法违约行为的情况下，个人还可以无条件撤回同意，并要求删除其个人信息。这一规定在知情同意权的基础上，进一步拓展了个人对其个人信息的自主权，是对“个人信息权”的深化落实。然而，在未明确区分个人信息与个人数据的前提下，删除权难以充分发挥其应有功能。一方面，个人数据在流通过程中常被多方处理和复制，初始数据处理者难以全面掌控个人信息的传播与存留，仅能删除自身掌握的数据副本，难以实现彻底的删除效果。另一方面，在人工智能大模型训练场景中，个人信息被抽象、编码并融合于模型内部形成“黑箱”，即便是模型开发者，也难以识别和删除其中具体的个人信息，从而导致删除权难以有效实施。

针对上述困境，我们必须从价值实现的角度重新审视删除权的适用范围。在“区分理论”的指导下，我们应着重保护个人信息，而非个人数据。这意味着，当个人行使其删除权时，法律应要求数据处理者删除那些能够直接或间接识别个人身份的信息，而不是那些经过处理、无法直接识别个人身份的数据。有学者指出，删除权的适用对象为个人信息，因此在判断是否应当删除某项数据时，应以其是否具备可识别性作为核心标准。[24]也就是说，只要流通中的个人数据不具备识别特定个人及特定人的可能性，就无需履行删除义务。这种删除义务在某种程度上也被视为数据主体的一种主动责任。例如，依据最小必要原则和目的限定原则，当信息收集目的已实现且无继续保存的合理理由时，数据运营者应主动删除所收集与存储的个人信息，以防信息处理活动超出必要范围。这一观点实际上对删除义务提出了更为严格的标准。需要强调的是，个人信息作为人格权保护的客体，一旦失去识别特定自然人的能力，其删除权便不再具备合理依据。

相比较而言，欧盟 GDPR 所使用的“个人数据”概念，深受其立法传统的影响，旨在对各类与个人相关的数据进行全面规制。该立法路径未对“个人信息”进行专门界定，是为了确保规则体系在多元成员国中的适用性和一致性。尽管在术语表述上存在差异，但欧盟立法所规制的“个人数据”实际上已覆盖了其他法域中“个人信息”的核心内容。欧盟采用不区分“个人信息”与“个人数据”的统一框架，虽然强化了隐私权保障，但由于其宽泛的定义和严苛的匿名化标准，实际抑制了数据流通效率，加重了企业的合规负担与技术适配成本。尽管欧盟通过后续的《数据法》尝试进行修补，但其核心的人权保护与数据经济化的冲突依然存在。

而我国在立法体系中尽管明确区分了《个人信息保护法》《数据安全法》《网络安全法》等多个并行法律，但他们各自承担着不同的制度功能。在此背景下，单纯依赖欧盟路径来解读我

国的《个人信息保护法》，并不能完全契合我国产业结构、平台生态以及数据要素市场建设的实际情况。某种程度上说，对欧盟立法模式的路径依赖，正是当前我国数据治理体系陷入“知情同意泛化”“数据要素僵化”等困境的深层原因之一。因此，法律规制已无法再依赖单一维度的权利保护逻辑，应当尽快打破“混同论”所塑造的理论僵局，而区分理论不仅有助于我们更精准地理解和适用删除权等相关权利，也为个人信息保护实践提供了新的阐释路径。一言概之，数据不应再被视为信息的另一种形态，而应作为一种独立的法律客体、具有独立功能定位的生产要素纳入制度设计，尤其要重新定位《个人信息保护法》为人格权保护的专属法律，回归其对信息识别价值的保障逻辑。同时，将《个人信息保护法》中涉及数据计算价值实现的相关内容，如数据流通、平台竞争秩序及资源控制等功能部分剥离出来，纳入以数据利用为导向的法治体系中进行规范。

注释：

① 参见龙卫球：《数据新型财产权构建及其体系研究》，《政法论坛》2017 年第 4 期。

② 例如，《网络安全法》将“网络数据”定义为“通过网络收集、存储、传输、处理和产生的各种电子数据”；《数据安全法》规定的数据是指“任何以电子或者其他方式对信息的记录”；《个人信息保护法》将“以电子或其他方式记录的与已识别或可识别的自然人有关的各种信息”均纳入“个人信息”范畴，导致数据和信息的概念相互交叉、难以区分。

③ 多数学者以数据要素化的需求为基础，主张为在数据价值创造中满足个人信息保护的法律要求，应将数据和信息区分开来。

④ 参见程啸：《论大数据时代的个人数据权利》，《中国社会科学》2018 年第 3 期。

⑤ 参见徐玖玖：《利益均衡视角下数据产权的分类分层实现》，《法律科学（西北政法大学学报）》2023 年第 2 期。

⑥ 参见武腾：《个人信息积极利用的类型区分与合同构造》，《法学》2023 年第 6 期。

⑦ 韩旭至：《信息权利范畴的模糊性使用及其后果——基于对信息、数据混用的分析》，《华东政法大学学报》2020 年第 1 期。

⑧ 参见梅夏英：《信息和数据概念区分的法律意义》，《比较法研究》2020 年第 6 期。

⑨ 参见张红：《我国法律文本中的“数据”：语义、规范及其谱系》，《比较法研究》2022 年第 5 期；王成：《个人信息民法保护的模式选择》，《中国社会科学》2019 年第 6 期。

⑩ 参见王利明：《敏感个人信息保护的基本问题——以〈民法典〉和〈个人信息保护法〉的解释为背景》，《当代法学》2022 年第 1 期。

⑪ 程啸：《个人信息范围的界定与要件判断》，《武汉大学学报》（哲学社会科学版）2024 年第 4 期。

⑫ 参见张新宝：《个人信息收集：告知同意原则适用的限制》，《比较法研究》2019 年第 6 期。

⑬ 参见李立丰：《〈个人信息保护法〉中“知情同意条款”的出罪功能》，《武汉大学学报》（哲学社会科学版）2022 年第 1 期。

⑭ 参见宋冬林、田广辉：《平台经济中数据垄断的根源、途径与治理策略》，《苏州大学学报》（哲学社会科学版）2023 年第 1 期。

⑮ 参见袁波：《必需数据反垄断法强制开放的理据与进路》，《东方法学》2023 年第 3 期。

⑯ 参见全国信息安全标准化技术委员会秘书处发布的《网络安全标准实践指南——网络数据分类分级指引》（TC260-PG-20212A）。

⑰ 参见林北征：《个人信息匿名化概括式立法的困境与完善》，《行政法学研究》2024 年第 6 期。

⑱ Robert M. Losee, “Information In A Data Collection: Models of Database and Library Quality,” *Journal of the American Society for Information Science*, vol.41, 1990.

⑲ Chang, W. L., Grady, N. “NIST Big Data Interoperability Framework: volumel, Definitions,” *National Institco of Standards and Technology*, October 21, 2019.

⑳ 参见周斯佳：《个人数据权与个人信息权关系的厘清》，《华东政法大学学报》2020 年第 2 期。

㉑ 参见杨芳：《个人公开信息爬取中侵权法与竞争法的互动》，《中国法律评论》2022 年第 6 期。

㉒ 参见程啸：《个人数据授权机制的民法阐释》，《政法论坛》2023 年第 6 期。

㉓ 参见丁晓东：《论数据携带权的属性、影响与中国应用》，《法商研究》2020 年第 1 期。

㉔ 参见王利明：《论个人信息删除权》，《东方法学》2022 年第 1 期。

编辑　李　梅　孙冠豪