数字时代隐私权的社会理论重构

余成峰*

内容提要 现代隐私法立足于个人主义、个人与社会二分以及个人信息概念的三大理论预设，汇聚为控制隐私与访问隐私两种核心范式，形塑了个人本位的隐私传统。数字时代背景下，伴随行动者、沟通模式和信息类型的变化，以及平台化、规模化等宏观结构转型，隐私的个人本位传统面临困境。从社会结构、社会功能、价值基础和法律概念四个方面考察，个人本位的隐私保护需进一步结合社会本位保护。立足中国国情，应积极探索个人本位保护与社会本位保护的融合，综合不同法律技术和监管工具，通过兼容并包、相互涵纳、内在制衡、协调统合的制度构建，最终形成商业市场、组织监管、风险治理、语境场景、网络制度、公共商谈模式在内的系统化隐私法律保护生态。

关键词 隐私权 个人信息保护 数字时代 社会理论 社会本位
DOI:10.14111/j.cnki.zgfx.2023.02.009

目 次

* 北京航空航天大学法学院、人文与社会科学高等研究院副教授，法学博士。本文系 2020 年度国家社科基金一般项目“第三波法律全球化的范式变迁研究”（项目批准号：20BFX008）的阶段性成果。

个人信息保护在当代遭遇挑战，核心根源在于数字时代背景下隐私权面临的规范性危机。现代隐私的个人本位与数字社会的运行逻辑存在矛盾，隐私侵权的发生机理和法律救济的个体机制发生错位。为应对技术与社会变革带来的系统性问题，隐私权的社会理论基础需要重构。

围绕数字时代的隐私权和个人信息保护，中外法学界与实务界已形成丰富的理论研究和制度探索成果。但是，从沃伦和布兰代斯 1890 年发表《隐私权》一文，到 1970 年代之后发展的公平信息实践原则（Fair Information Practice Principles，简称 FIPPs），再到晚近以欧盟《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）为代表的国别与区域性立法，已有研究和立法主要囿于 19 世纪的古典社会理论范式，遵循个人本位的权利保护和私人诉讼的救济思路。[①] 尽管相应的法律与监管措施层出不穷，但隐私保护却陷入制度供给不足和供给过度的双重悖论，乃至出现隐私的死亡与终结这样的悲观论断。[②] 鉴于此，本文通过分析现代隐私法的个人本位传统，揭示数字时代背景下隐私保护面临的深刻困境，进而通过重构隐私权的本体论和价值论基础，重塑隐私权的社会本位意涵，为构建数字时代多层次、分化制衡的隐私保护制度体系提供新的社会理论框架。

一、个人本位的现代隐私法

（一）三大理论预设：隐私个人本位的法理基础

现代隐私法立足于个人主义、个人－社会二分以及个人信息概念三个方面的理论预设，形成个人本位的隐私传统。

1. 基于个人主义的理论预设

现代隐私以古典自由主义的自主观念和个人主义规范论为基础。第一，隐私保护的是个体自治与独立，它预设侵犯隐私损害的是个人自主权，通过对隐私的控制可以重建这一自主权。这在规范上预设了一种原子主义的法律人格，隐私被化约为一个私人性的空间领域，在其中，一个人拥有作出任意选择的无限可能性。现代隐私因此尤其推崇隔离与自足，隐私主体被理解为“自决的、无负担的、个人的，仅仅与他人通过选择发生联系的形象”[③]。易言之，现代隐私立足鲜明的个人主义传统，保护个人的主观性法益，抵御对个人内在的伤害。第二，由于预设隐私人格在规范上具有道德自主性与自决性，因此进一步预设个人拥有充足的理性，可以有效行使其权利。[④] 隐私主体被假定可以理性评

① *See* Samuel Warren & Louis Brandeis, *The Right to Privacy*, Harvard Law Review, Vol.4:193, p.193 (1890); Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, Stanford Technology Law Review, Vol.1:1, p.1 (2001); Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, Seton Hall Law Review, Vol.47:995, p.995 (2017).

② *See* Michael Froomkin, *The Death of Privacy?*, Stanford Law Review, Vol.52:1461, p.1461 (2000).

③ Colin Bennett, *In Defence of Privacy: The Concept and the Regime*, Surveillance & Society, Vol.8:485, p.486 (2011).

④ *See* Sebastian Benthall & Jake Goldenfein, *Data Science and the Decline of Liberal Law and Ethics*, at https://ssrn.com/abstract=3632577 (Last visited on March 25, 2023).

估当下和潜在的未来状况，计算隐私披露的成本与影响。[⑤] 这进而构成隐私法上至为重要的知情同意原则的法理基础：预设个人拥有充分理性，因此一旦获得控制权，个人就可以根据其偏好作出最有利的隐私决策。[⑥] 实践中，隐私权因而主要落实为“控制个人信息使用的个人权利”[⑦]。第三，隐私被定位为一种与世界隔离和对抗的个人权利概念，隐私保护的目的是为个人的涉己行动创造不受干涉的自由区域。隐私时刻警惕公共权力对私人领域的入侵，正因如此，隐私的规范理想不只是实现信息的个人控制，更是将之作为政治自由价值的基础。

2. 基于个人—社会二分的理论预设

现代隐私建立在一系列社会理论的预设之上，塑造了特殊的社会世界观。第一，在社会结构层面，它预设了一个二元分化的世界，即将世界区分为隐私与公共两个领域，在私和公之间划分出一条清晰的分界线。[⑧] 隐私隶属于个人空间，一旦进入社会空间，隐私期待则相应消失。在私人领域，个人拥有隐藏或分享信息的决策权，以此控制外界的访问；而一旦暴露于公共空间，则意味着自动放弃了对于隐私的主张。第二，在社会功能层面，隐私被视为实现各种个人行动目标的基本工具。个人正是借助不同的隐私策略自主调节私人与公共的界线，通过创设特定的私人地带，营造行动的自由空间。[⑨] 在这一功能视角下，个人与社会形成对立的关系。个人和社会边界的持续调整来自个人的隐私决策，并由此成为私域与公域分化和对峙的基础。第三，在社会媒介层面，个人成为信息沟通和保护的基本单元，预设个人拥有特定的个人信息，在个人隐私、个人信息与个人身份之间形成相互映射、相互识别的关系。[⑩] 通过塑造隐私人格，隐私被固定于个人领域，以此确立隐私的定义和范围。借助隐私这一媒介，个人可以有效抵挡社会侵入，获得自由进入和退出社会沟通网络的能力，并以此成为社会秩序运行的节点。

3. 基于个人信息概念的理论预设

现代隐私法以个人为本位，通过个体化策略进行隐私权的解释与应用。个人拥有个人信息并且个人信息有遭受侵害的可能，这种理解一直主宰着隐私权的实践。第一，现代隐私理论认为应由个人来决定何者归属于个人，何者归属于公共。[⑪] 这一理论决定了

---

⑤ *See* Paul Dourish & Ken Anderson, *Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena*, Human-Computer Interaction, Vol.21:319, p.326 (2006).

⑥ *See* Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, A Journal of Law and Policy for the Information Society, Vol.6:425, p.434 (2011).

⑦ Paul Schwartz, *Internet Privacy and the State*, Connecticut Law Review, Vol.32:815, p.820 (2000).

⑧ 参见［美］丹尼尔·沙勒夫：《隐私不保的年代：如何在网络的流言蜚语、人肉搜索和私密窥探中生存》，林铮颢译，江苏人民出版社 2011 年版，第 168 页。

⑨ *See* Stephen Margulis, *On the Status and Contribution of Westin's and Altman's Theories of Privacy*, Journal of Social Issues, Vol.59:411, p.422 (2003).

⑩ *See* Robert Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere*, Duke Law Journal, Vol.67:981, p.1004 (2018).

⑪ *See* Dorothy Glancy, *The Invention of the Right to Privacy*, Arizona State Law Journal, Vol.21:1, p.21 (1979).

隐私保护主要依托私人执行机制，主要借助个人自主控制与诉讼。⑫ 隐私保护因此依赖个人的判断和决策，依靠个人识别以及抵制个人信息领域遭受侵害的能力。⑬ 各类隐私法保护工具的核心要义即“帮助个人理解和控制那些直接有关他们的信息”⑭。第二，正因如此，个人信息成为当代隐私规制的焦点，个人信息成为隐私保护的基础概念。法律实践中，正是通过区分个人信息与非个人信息，隐私的保护范围不断得到确定和调整。申言之，隐私法通过个人信息与非个人信息的二元区分来划定个人和社会的领域，厘定隐私保护的对象，明确个人隐私的自主控制范围。第三，通过将非个人信息排除在保护范畴之外，为隐私的自主控制设置合理边界，以避免将有限的监管资源投入到保护范围无限的信息沟通中去。同时，通过借助个人同意来判断合法和非法的个人信息使用，隐私规制的负担被有效分配与转移给个体，隐私保护因此简化为个人的知情选择行为，隐私的个人本位传统由此进一步强化。

（二）控制与访问：个人本位的两种隐私范式

基于上述三个方面的理论预设，最终汇聚形成控制隐私和访问隐私两种核心范式。以阿兰·威斯汀（Alan Westin）为代表，控制隐私从形式、主观与积极自由的层面，强调个人对有关自己的信息、知识和决策的控制。⑮ 以露丝·嘉维森（Ruth Gavison）为代表，访问隐私则从实质、客观与消极自由的层面，界定了个人在完全无法被他人访问时所拥有的完美隐私状态。⑯ 两大范式共同立足于个人本位的视角，横跨从心理系统到社会系统的隐私梯度轴线，⑰ 通过将个人置于社会语境虚化的抽象背景下，从经验和规范两个维度，为个人本位的隐私法理论提供了整全的正当性说明。在两种范式的共同加持下，隐私浓缩为个人自主控制外界访问的含义。隐私由此分离于社会，成为个人自主处分的概念。申言之，无论控制范式还是访问范式，都采取了将社会分解为由孤立个人构成的意象。隐私的首要目标，即是在个人与社会之间确立起严格的分界。

二、个人本位隐私传统的困境

在数字技术和平台商业模式的共同驱动下，微观的行动者、沟通模式与信息类型正在悄然发生变化，宏观社会结构经历剧烈的转型，个人主义、个人－社会二分和个人信息

⑫ *See* Chris Berg, *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change*, Springer, 2018, p.50.

⑬ *See* Shaun Spencer, *Reasonable Expectations and the Erosion of Privacy*, San Diego Law Review, Vol.39:843, p.845 (2002).

⑭ Joshua Fairfield & Christoph Engel, *Privacy as a Public Good*, Duke Law Journal, Vol.65:385, p.413 (2015).

⑮ *See* Alan Westin, *Privacy and Freedom*, Atheneum, 1967, p.9.

⑯ 嘉维森认为，一个人（X）完全无法被他人访问时，拥有完美的隐私。这可以分解为三个独立因素：没有人知道任何有关 X 的信息（秘密），没有人对 X 投以任何注意力（匿名），没有人可以在物理上访问 X（独处）。*See* Ruth Gavison, *Privacy and the Limits of Law*, The Yale Law Journal, Vol.89:421, p.423 (1980).

⑰ 根据从孤立个人到社会参与的梯度轴线，控制隐私可进一步细分为心智隐私—决策隐私—结社隐私—行动隐私，访问隐私可进一步细分为身体隐私—空间隐私—沟通隐私—专有隐私。*See* Bert-Japp koops et al., *A Typology of Privacy*, The University of Pennsylvania Journal of International Law, Vol.38:483, p.484 (2017).

概念作为现代隐私权的社会理论预设受到挑战，现代隐私的个人本位传统面临深刻困境。

（一）行动者：个人主义理性的困境

传统隐私理论预设行动者具有足够的计算伤害或回报概率的能力，假定个人可以自由表达自己的隐私偏好，其行动能够准确反映自己的隐私偏好。但是，晚近的行为社会科学研究揭示，真实行动者往往是“天真、不确定和脆弱的人”⑱。有限理性限制个人获取、记忆与处理所有相关信息，因此往往依赖简化的思维模型和思维捷径。实践中，个人往往对远期与当下事件形成区别对待，存在过度自信、理性忽略、现状偏见和行为异常等状况。⑲ 进言之，数字时代的隐私问题具有概率化特征与不可预测性，行动者囿于不完全信息和有限的认知能力，无法在决策当下知晓所有相关因素，严重的认知问题削弱了“隐私的自我管理”⑳，“在这种情况下，同意变得没有意义”㉑。一方面，海量数据的相互关联使个人无法全面评估同意数据收集的潜在成本；另一方面，个人也无法预测进一步会有何种信息被发现，因此无法确知自己披露的信息在与其他数以亿计的数据点结合时，将会发生何种后果。这些事实使个人主义的隐私理性成为一个本质上有缺陷的概念。

“自由的行使可能限制自由，控制的行使可能限制控制。”㉒ 行动者不仅面临有限理性的约束，也陷入通过理性自主放弃隐私的悖论。实践中，个人往往会接受各种标准合同条款或默认隐私政策，倾向于保持信息披露最大化的设置。各类大型平台不断将个人变成排名和评级的对象，㉓ 个人迫于平台使用的便利，往往通过隐私决策削弱对于隐私的控制。旨在增强个人自主的隐私控制，反而可能进一步导向隐私的自我披露。隐私的自主放弃不再只是出于认知能力的不足，还是工具理性计算的结果。

个人主义的困境不仅来自隐私主体，也来自隐私侵犯主体的变化。各类大型平台通过影响社会实践来强化其市场地位，成为数字社会的超级行动者。新的数据处理环境和其他影响与限制隐私选择的架构，正在不断消除隐私个人控制的可能性。由于普遍依赖思维捷径，个人的隐私决策很容易受到默认设置与网络环境设计的影响，平台的超级助推通过架构设计，可以将用户选择引导到平台偏好的方向。㉔ 在这个过程中，平台可以巧妙地通过游戏化的消费主义来攫取用户数据。申言之，作为超级行动者的平台通过高度不对称的信息环境来操纵个人的隐私选择，利用私有市场持续囤积个人信息，并通过大规模社会实验获得对个人的绝对优势。

---

⑱ Alessandro Acquisti, *Privacy and Human Behavior in the Age of Information*, Science, Vol.347:509, p.514 (2015).

⑲ *See* Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us about Privacy?*, in Alessandro Acquisti & Stefanos Gritzalis eds., Digital Privacy: Theory, Technologies, and Practices, CRC Press, 2007, p.369-373.

⑳ Daniel Solove, *Privacy Self-Management and the Consent Dilemma*, Harvard Law Review, Vol.126:1880, p.1880(2013).

㉑ Julia Lane et al. eds., *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, Cambridge University Press, 2014, p.61.

㉒ Adam Moore, *Privacy Rights: Moral and Legal Foundations*, Pennsylvania State University Press, 2010, p.17.

㉓ *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, Washington Law Review, Vol.89:1, p.3 (2014).

㉔ *See* Karen Yeung, *“Hypernudge”: Big Data as a Mode of Regulation by Design*, Information, Communication & Society, Vol.20:118, p.232 (2017).

传统隐私关注个人，而不是人的类型。与之相反，当前的大数据技术并不聚焦于特定个体，而是聚焦于大规模人群或者说所有人。由此形成的群体隐私风险与侵害，难以追溯特定的侵权行为人和侵权受害者。在这种背景下，即使是完美的知情和理性，个人“也只能控制自己的数据，无法影响大数据算法所运行的信息海洋”㉕。易言之，新的数字时代，算法主要根据平台感兴趣的群体而不是个体进行决策，主要依据相应场景的群体行为特征知识，构建各类临时性的算法群组与标签类别，个人只是作为数据点被化约性地纳入其中。㉖

（二）沟通模式：个人主义控制的挑战

从工业时代以来，围绕信息收集和处理就已开发出复杂的分类机制，以解决组织与个人之间的信息不对称问题。数字时代借助新的数据采集、聚合和挖掘技术，进一步瓦解了个人隐私控制的可行性。数字网络正转型为感应网络，围绕始终在线的移动设备，以高度颗粒化的信息流方式进行持续收集和传输。数字沟通采取软监控与软家长的作风，“利用认知约束来鼓励顺从，同时保持选择的错觉”㉗。基于在线用户连续的交互反馈循环，算法控制可以通过各种微妙而隐蔽的方式运行。这个过程结合了机器学习和超级助推技术，㉘ 因而不会导致“可能激发道德愤怒和产生反制力量的发自内心的压迫感……数据提取旨在尽可能无缝与轻松地进行”㉙。正如斯科特·拉什（Scott Lash）所概括，信息权力正变得本体化，权力不再是通过对意义的霸权控制，而是通过群体内化的技术表现。㉚

分类和信号是克服组织与个人信息不对称的两种对反手段，与工业时代的分类经济不同，数字时代正迈向新的“信号经济”。如果说分类经济的沟通模式是自上而下的数据采集，信号经济的要义则是“通过精准阈值设定诱惑与刺激，让个人自愿贡献自己的信息”㉛。平台架构的巧妙设计，可以将个人的隐私披露自动整合进感应网络，通过精准的供应链管理技术，有效降低隐私收集的不确定性。申言之，平台正同步推进自上而下的数据攫取和自下而上的自主贡献。其中，隐私监控采取了一种新颖的众包形式，充分调动个人参与到信息收集和验证的劳动密集型过程。㉜ 新的沟通模式致力于塑造隐私披露

㉕ Joshua Fairfield & Christoph Engel, *supra* note 14, 27.

㉖ 在这种趋势下，“数字集体标识符破坏了个人、身份和隐私之间的长期联系”，“人的去个体化”呼唤新的“类型隐私”观念。*See* Brent Mittelstadt, *From Individual to Group Privacy in Big Data Analytics*, Philosophy & Technology, Vol.30:475, p.476 (2017); Anton Vedder, *KDD: The Challenge to Individualism*, Ethics and Information Technology, Vol.1:275, p.275 (1999).

㉗ Ian Kerr et al., *Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent*, Personally Yours, Vol.6:1, p.11 (2006).

㉘ *See* Mireille Hilderbrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, Theoretical Inquiries in Law, Vol.20:83, p.109 (2019).

㉙ Salome Viljoen, *A Relational Theory of Data Governance*, Yale Law Journal, Vol.131:573, p.573 (2021).

㉚ *See* Scott Lash, *Power after Hegemony: Cultural Studies in Mutation?*, Theory, Culture & Society, Vol.24:55, p.55-78 (2007).

㉛ Colin Bennett, *supra* note 3, 489.

㉜ *See* Julie Cohen, *The Surveillance-Innovation Complex: The Irony of the Participatory Turn*, in Darin Barney et al. eds., The Participatory Condition in the Digital Age, University of Minnesota Press, 2016, Forthcoming, p.6.

的选择环境，其要旨是将个人的隐私决策自发导向到平台偏好的选择架构之上。正因如此，个人现在不只是被平台挖掘数据，也相互激励和竞争性地披露隐私，以换取各种红利或避免不利。质言之，“信号经济”对个人隐私的威胁，与传统隐私法关注的个人信息采集、聚合与分类的威胁截然不同。

实践表明，算法技术已形成新的、高度精细的评估受众和预测受众的方法，从而将隐私采集转化为最适合数字经济商业模式开发的形式。以行为广告、超级助推、黑暗模式等为例，这些数字技术并不遵循传统隐私的定位，无需识别特定的个人，算法技术只需要依靠一些容易收集的信息，就可以根据相应的统计学模式去定位所有相关人。易言之，由于各类算法嵌入各种变量、相关性和推断技术，算法的概率解析因此可以提供意想不到的观察与推断个人的方式，隐私的个人主义控制遭遇深刻挑战。[33]

（三）信息类型：个人信息概念的局限

许多研究者都注意到大数据技术正使个人信息与非个人信息的二元区分失去意义。[34] 首先，大数据时代的信息愈加具有外溢效应、网络效应和涟漪效应。[35] 新的数字技术可以利用“智能”环境中的任何信息，所有信息都可能在主观预期影响或客观结果影响的层面与个人相关联（relate to）。[36] 其次，在大数据环境下，即使个人没有被“识别”（identify），仍然可能被“触及”（access），数字技术“仍然可能针对他们的特征和活动的细节进行全面记录，并由此进行间接推断与预测”[37]。因此，个人难以预测和排除所有可能从特定信息项的可用或缺失中得出的三阶或四阶推论，因此无法对隐私伤害形成明确认知。最后，大数据算法分析技术的特点导致零散的个人身份信息出现贬值。数字画像现在主要由行为数据，而不是个人数据提供。行为数据的庞大规模以及算法技术的复杂性，挑战了传统个人信息概念的有效性。[38]

新型数字技术正将关注焦点从传统的个人信息转向群组信息。首先，当代的数字画像技术通常与群组建构（具有 x、y 和 z 特征的人群）而不是个人识别相关，算法主要根据不一定准确代表任何特定个人的可测量指标而将人群分别归类，这些信息通常不是

---

[33] 归入特定群组并因此强加于个人的意义不一定反映他的自我理解。*See* Deborah Lupton, *The Commodification of Patient Opinion: The Digital Patient Experience Economy in the Age of Big Data*, Sociology of Health & Illness, Vol.36:856, p.856-869 (2014).

[34] *See* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, Northwestern Journal of Technology and Intellectual Property, Vol.11:239, p.258 (2013).

[35] *See* Nadezhda Purtova, *Property Rights in Personal Data: Learning from the American Discourse*, Computer Law & Security Review, Vol.25:507, p.507 (2009).

[36] *See* Nadezhda Purtova, *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, Law, Innovation and Technology, Vol.10:40, p.56 (2018).

[37] Solon Barocas & Helen Nissenbaum, *Big Data's End Run around Anonymity and Consent*, in Julia Lane et al. eds., *supra* note 21, 46。学者建议用“可触及性”取代“可识别性”的要求。*See* Maša Galič & Raphaël Gellert, *Data Protection Law Beyond Identifiability? Atmospheric Profiles, Nudging and the Stratumseind Living Lab*, Computer Law & Security Review, Vol.40:1, p.13 (2021).

[38] *See* Brent Mittelstadt & Luciano Floridi, *The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts*, in Brent Mittelstadt & Luciano Floridi eds., The Ethics of Biomedical Big Data, Springer, 2016, p.445-480.

“个性化和情境敏感的，而是块状的”[39]，这导致许多算法处理过程难以纳入“个人信息”保护法的范畴。其次，个人信息的主要作用在于定位相关的群体类别，重要的是从个人信息中推断出的群组信息。平台对于某人是谁并不存在特殊兴趣，因为即使没有这些个人信息，平台为个人定制服务的能力也不受任何影响。最后，传统的个人信息类别（例如姓名、地址）在算法分析中越来越不相关，因为算法主要根据行为、偏好和其他特征进行概率化的群组分类，从而无需针对个人进行具体的身份识别。数字广告商关心的主要不是向谁推送广告，而是其广告能否到达目标市场。广告商并不识别群组（例如市场细分）中的特定成员，而只需根据算法分类进行有效的市场定位与精准投放。重点是揭示具有特定偏好或行为的群组成员的相关性，而不是识别个人身份。[40]

“个人信息和非个人信息的边界不是固定的，而是取决于技术。”[41] 数字时代，平台能够在短时间内筛选、分类海量数据，将信息处理的硬件配置与用于识别模式、将模式提炼成预测的机器学习技术相结合，通过不断调整模式并提炼预测以回应新的数据，由此形成高度数据密集型的平台信息。如果说传统隐私主要关注个人信息，这些个人信息通常被置于具有确定边界的单一信息系统中处理，而在当下，个人信息则被纳入互联的信息系统，这些系统高度网络化，个人信息在这一互联系统中通过不同方式被进行连续化的处理。[42] 在此过程中，平台往往会利用概率推断作为获取额外信息的桥梁。伴随新算法模型的应用，个人的信息表征会不断演变，并根据新的数据输入不断调整其模式。申言之，平台不再只是收集个人信息，同时也在创造个人信息，这些信息不再只是原始的个人隐私，而是平台开发者关注的涉及消费与注意力模式的人工生成品。

现代隐私法采取全有全无的保护路径：信息要么是个人信息（促发保护机制），要么不是个人信息（无法促发保护机制），而不能是介于两者之间的状态。但事实上，“这种二元性与任何信息都有可能影响人们的世界是不一致的”[43]。首先，新兴数字技术现在可以从已知信息推断新的信息，例如通过分析他人在社交网络中披露的信息和行为，或通过交叉引用“去识别化”的数据集而得出相关的敏感信息。[44] 其次，个人信息不再只是“个人私有和排他性的领域，而是与所有人相关”[45]。个人信息每天都被大量不同的使用者频繁使用，在超越个人知识与控制的不同领域处理，“数据有时作为个人数据，有时

---

[39] Scott Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, Northwestern University Law Review, Vol.105:1153, p.1178 (2011).

[40] *See* Luciano Floridi, *Open Data, Data Protection, and Group Privacy*, Philosophy & Technology, Vol.27:1, p.1-3 (2014).

[41] Daniel Solove & Paul Schwartz, *The PII Problem: Privacy and a New Concept of Personally Identificable Information*, New York University Law Review, Vol.86:1814, p.1846 (2011).

[42] *See* Stefan Strauß, *Privacy and Identity in a Networked Society: Refining Privacy Impact Assessment*, Routledge, 2019, p.231.

[43] Nadezhda Purtova, *supra* note 36, 80.

[44] *See* Deirdre K. Mulligan, Colin Koopman & Nick Doty, *Privacy is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy*, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, Vol.374:1, p.2 (2016).

[45] Joshua Fairfield & Christoph Engel, *supra* note 14, 24.

作为非个人数据，我们根本无法预测两者中的哪一个会发生”[46]。最后，在这种趋势下，个人信息和非个人信息的边界无法提前确定，而是取决于未来与不可预测的事件。由于任何信息都可能涉及个人，识别个人信息与非个人信息变得日益困难，隐私法可能转变为万物法。质言之，伴随个人信息概念的不断扩展和泛化，当前以个人信息概念为中心的隐私保护范式面临严峻挑战。

（四）大转型：个人－社会二分结构的变迁

不仅是微观的行动者、沟通模式与信息类型发生转变，致使个人本位的隐私保护受到冲击，数字时代的宏观社会结构也正在经历平台化、规模化等大转型，这动摇了现代隐私立足的个人－社会二分的理论预设，从而腐蚀了个人隐私保护可以借助的社会结构条件的基础支撑。

社会结构的平台化，是指平台的数据化和算法化架构，通过对社会基础设施与个人选择架构的改造，可以实现覆盖全社会的软监控和软家长式作风的渗透。通过对信息基础设施与网络生态系统的深度干预和调配，平台可以提取个人的行为线索并在潜意识层面塑造相应的情感与动机，从底层架构对个人的情绪、动机和偏好这些预认知功能进行调制，从而在全社会进行广泛的预认知激活与操纵。正如有的研究者所说，它“旨在增强内容定位和行为营销能力的监控组合，创建强大且易于工具化的刺激响应反馈循环”[47]。当前的平台生态往往涉及众多数据控制者与处理者共享数据集，这些数据被用于各种不同并且经常是模糊的目的，数据处理过程往往是自动化的。通过构建各类集成信息系统，平台在为用户提供服务的同时，也同步实现对用户个人信息的全面追踪。平台化社会结构的运作逻辑不再只是对个人隐私的窥探，也寻求算法目标的最优化调适。平台立足于算法的模式化驱动，个人的数字画像被吸纳到平台的总体运行目标中，并在促进目标最优化调适的方向上持续助推个人的隐私选择。

传统隐私理论预设个人可以在独立的私有空间内自主决策和行动，未能充分考虑社会结构的复杂实际。数字社会尤其具有高度复杂的特征，隐私的个人管理难以回应数字时代的规模化问题。与针对个人的隐私侵犯不同，当前的数字实践主要在群体规模化的层面运行。算法决策可以在不同情况下广泛共享，由此形成系统性与累积性的社会效应。这种背景下，个人的选择难以从具体的规模化社会语境中抽离出来，个人的隐私决策往往只能在有限的选择集中作出，“只要我们与他人互动，其他人的行为就会随时影响我们开放的选项范围”[48]。当前的问题主要不是孤立的个人隐私侵犯，而是各类数字算法基于规模化运作形成的系统性社会歧视和排斥。个人本位的隐私保护，难以在社会结构层面表征数字时代的规模化特征。

数字时代的另一个重大变化，是私人领域与公共领域都在经历深刻的结构转型。通

[46] Bert-Japp Koops et al., *supra* note 17, 13.

[47] Julie Cohen, *Internet Utopianism and the Practical Inevitability of Law*, Duke Law & Technology Review, Vol.18:85, p.88 (2019).

[48] Karen Yeung, *supra* note 24, 14.

过控制各类公共信息和个人信息，私人领域的公共化与公共领域的私有化同步发生，公共领域和私人领域的关系正在发生戏剧性的颠倒。社会理论研究已揭示，在社会明确期待保护的（私人）信息与明确认为不需保护的（公共）信息之间，不可避免存在着广阔的灰色地带，而各种数字技术正不断侵入这些灰色地带，持续改变社会的隐私期待。[49] 平台不仅通过改变个人的可访问性来影响隐私，同时也通过改变隐私规范本身来影响隐私。质言之，数字时代破坏了传统公与私的二分结构，既有的公私边界正在坍塌，个人隐私立足的公私二元机制面临深层危机。

综上所述，传统隐私立足的个人主义、个人－社会二分与个人信息概念的理论预设遭遇深刻挑战，当前需从社会理论视角出发，进一步深化对数字时代隐私性质、存在形态与保护模式的认识，探索数字时代隐私保护的新方向。

三、社会本位隐私保护的正当性

数字时代背景下，隐私的社会本位保护具有应对社会结构转型的必要性，而从隐私权的本体论和价值论视角考察，同样也可以提供隐私社会本位保护的正当性证明。运用社会理论分析工具，则可以从功能视角揭示隐私权和个人信息概念的社会建构性。

（一）社会结构：高度流动与复杂连带

数字技术变革推动社会结构的深刻转型，社会关系呈现高度网络化与流动化的特征，各种实体形成相互依赖、复杂连带的生态体系。

第一，媒介技术的变化。新的数字媒介强调无缝追踪、行为和注意力模式的细粒度测量、连续数据流的提取以及将数据流配置为最适合算法分析与商业开发的形式。在这种背景下，个人信息收集和处理已成为一种持续不断的状态。各种智能移动设备通过专有接口与服务协议，采集各类高度精细的信息流，并将之传输到强大的专有机器学习系统。在这种媒介技术环境中，通常是以算法系统目标最优化的方式提炼和加工个人信息，以高度颗粒化的方式将个人的多变性转换为模式化的概率梯度，进而在群组聚合的意义上整合为可计算、预测化与营利化的对象。[50] 易言之，当代数字媒介技术的取向不是纯粹的个人隐私，而是个人隐私在商业模式中的表现，通过促成隐私的统计学建构，以群体规模方式进行管理和干预。如果说传统隐私侵害发生于个人层面，那么当代隐私侵害则在结构层面呈现。

第二，信息结构的转型。首先，大数据本质上是社会化的信息关系：关于某人的信息，同时也是关于他人的信息。大数据技术的复杂性与规模性，使我们难以准确区分个人信息的边界。实践中，个人信息在数据产业链上下游广泛使用，二次和三次用途变得常见；互联网公司的频繁合并或联盟关系导致数据库大量共享，涉及的人口群体数量尤

[49] *See* Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America*, Vintage Books, 2001, p.60-61.

[50] *See* Julie Cohen, *Law for the Platform Economy*, UC Davis Law Review, Vol.51:133, p.143 (2017).

其多。个人信息不断被吸纳整合为聚合数据库的内容，个人信息与公共信息的边界不断模糊化。其次，信息结构形成愈益复杂的连带性。由于越来越多的个人持续提交信息，因此在技术上也就有越来越大的概率去识别任何仍未披露隐私的个人。长时间以及从不同来源积累的数据对整个社会释放透明化效应，从而以个人难以预见的方式侵害隐私。质言之，在新的信息结构下，隐私保护不再仅仅关涉个人，同时也与整个社会的技术、商业模式以及权力运行机制相关联。[51]

第三，社会关系的调整。现代隐私凸显原子化的个人形象，强调孤立和隔离。而数字时代的社会关系愈益流动化、液态化，以数据“流”的形式存在。[52] 隐私不再仅仅是关于个人如何控制访问的问题，也是关于信息如何流动和连带的问题。[53] 首先，在新的社会背景下，某一个人的信息披露决策会深刻影响其他个人，即使只有一小部分人披露隐私，也可以将隐私选择的后果强加给大多数人。实践中，社会优势群体也可能作出有利于自身的隐私决策，并由此损害其他弱势群体的隐私利益。其次，数字时代正推动一系列新的社会行动者进入相关场域。在这一趋势下，信息披露者、控制者、处理者与接收者的社会关系链条变得高度复杂，形成众多在法律上难以准确定位身份和责任的主体。进言之，数字时代的社会关系主要不是个人的简单互动，而是个人作为各类组织、群组和群体的成员与角色，作为临时节点，嵌入具有高度流动性的复杂关系网络。

第四，社会生态的演变。当前隐私保护面临的是新型社会生态。首先，具有不同功能和角色的实体参与到各类信息技术系统中，例如系统操作者、算法开发者、硬件制造者、应用或服务提供商等。除了这些内部实体，还包括各种第三方外部实体。这些实体和系统相互渗透还可能产生各类无法预料的不兼容。[54] 其次，这里不仅涉及各类实体和信息系统，还牵涉复杂的技术设施、商业实践、文化情境与社会行动者相互依赖的生态关系。[55] 隐私问题涌现于社会生态层次（技术、制度与商业模式），而不只是个人层面（入侵住宅、私拆信件、偷听对话）。传统隐私主要处理个人－个人、个人－组织、个人－国家等二元对立关系，而在新的社会生态下，平台企业等已不只是外在于个人隐私的侵犯主体，同时成为隐私保护重要的技术中介和组织环境。

（二）社会功能：作为社会公共品的隐私

隐私不只是保护个人权益，也承担着重要的社会功能，为现代社会的互动沟通和系统运作提供基础支撑。正因如此，隐私具有超越个人本位的社会公共品维度。

第一，隐私作为个人的社会互动机制。传统隐私被视为一种孤立和隔离的概念，而

---

[51] 参见王锡锌：《个人信息国家保护义务及展开》，载《中国法学》2021 年第 1 期，第 154 页。

[52] 对于个人，“社交网络正在成为追求个人目标的条件……如果一个人不可见和不可接近，社会就会很容易忘记你”。*See* Felix Stalder, *Autonomy beyond Privacy? A Rejoinder to Colin Bennett*, Surveillance & Society, Vol.8:508, p.510 (2011).

[53] *See* David Lyon, *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, Routledge, 2002, p.19.

[54] 没有一个人可以“掌握整个系统或跟踪所有对其组成部分做出贡献的个人”。*See* Helen Nissenbaum, *Accountability in a Computerized Society*, Science and Engineering Ethics, Vol.2:25, p.5 (1996).

[55] *See* Beate Roessler & Dorota Mokrosinska, *Social Dimensions of Privacy: Interdisciplinary Perspective*, Cambridge University Press, 2015, p.51.

在社会理论视野下，隐私是个人间关系的函数，隐私的焦点是人际沟通与社会互动。[56] 隐私的重要功能是通过人际边界的调整，反向促进社会互动，换言之，没有隐私也就没有互动。[57] 正是在这个意义上，“隐私的重要性在于构成人际关系的基础，而不是促成个人社会”[58]。现代隐私强调个人的自主意志，而晚近研究则揭示个人自主是社会塑造和具身经验的产物。个人生活在由各种关系、实践与信仰包裹的网络中，是社会网络塑造了个人隐私的形态。概言之，在社会功能视角下，隐私并不意味着孤立。作为自我与他者的界线，隐私恰恰是通过社会互动和沟通的过程形成。隐私保护的不只是个人身心，而是通过对个人身心系统私密性与敏感性的保护，反向促进社会互动机制的繁育。

第二，隐私作为信息控制的社会制度形式。隐私的重要功能是处理信息隐藏与信息沟通的平衡关系。换言之，隐私是对人际信息流动与交换程度的管理，意在通过对信息连接和信息断开的合理规制来平衡这种张力，防止信息过度链接与识别对社会沟通进程的破坏。因此，在社会功能视角下，隐私不只是个人议题，同时也涉及社会信息控制与信息系统的设计特性。社会沟通系统的状态以及支配信息沟通的信息规则决定着隐私保护的具体参数。特别在数字时代背景下，数据可访问性不断嵌入社会技术系统的默认设置；信息的认证功能不断深入平台基础设施的核心；数据驱动的技术架构正在深刻改变社会沟通环境。在此意义下，数字时代隐私的焦点不只是如何保护个人控制的权利，更是如何设计和维护更合理的社会信息沟通系统的问题。

第三，隐私作为社会系统功能分化的要义。个人与社会紧密关联，如果说隐私的一阶效应指向个人，二阶效应则是对社会系统功能分化运作的支持。换言之，隐私不仅保护个人，同时也保护作为个人自治构成条件的社会结构本身。[59] 在社会系统论视野下，隐私乃是防止功能分化的社会系统迈向全能主义社会的基础手段。社会系统的功能分化，既是隐私成立的条件，也是隐私保护的核心目标。由隐私保障的社会功能分化排除了特定社会系统的代码扩张和功能蔓延，从而维持了功能分化社会系统的边界张力。[60] 概言之，在社会功能视角下，隐私的冲突不只是发生于人与人之间，同时也发生于不同的社会系统之间（互动系统、组织系统和功能子系统）。隐私的状态不仅取决于个人，也取决于不同社会系统的运作状态和功能表现。

第四，隐私作为社会公共品的形式。隐私之“私”，始终以预设“公共”作为前提。[61]

---

[56] *See* Stephen Margulis, *Privacy as a Social Issue and Behavioral Concept*, Journal of Social Issues, Vol.59:243, p.249 (2003).

[57] 奥特曼认为，隐私具有三个功能或目标：（1）人际界限的调节；（2）人际角色的发展和管理以及与他人打交道；（3）自我观察和自我认同。*See* Irwin Altman, *The Environment and Social Behavior*, Brooks/Cole Publishing Company, 1975, p.22.

[58] Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, 1995, p.69.

[59] *See* Dorota Mokrosinska, *Privacy and Autonomy: On Some Misconceptions Concerning the Political Dimensions of Privacy*, Law and Philosophy, Vol.37:117, p.123 (2018).

[60] *See* Katayoun Baghai, *Privacy as a Human Right: A Sociological Theory*, Sociology, Vol.46:951, p.952-957 (2012).

[61] 隐私“只有在另一极同时存在，并且在两个领域互动和互赖时才能存在”。*See* Sebastian Sevignani, *Privacy and Capitalism in the Age of Social Media*, Routledge, 2015, p.118.

和环境保护、安全、道路与国防一样，隐私也具有公共品属性。隐私既无法由个人单独生产和保护，也不存在利用上的竞争性和受益上的排他性。正是由于隐私指向一种服务全社会福利的公共品功能，这使得个人往往既缺乏能力也欠缺动机来保护隐私。[62] 特别是在数字时代，个人的隐私保护已经完全无法脱离整体数字环境的隐私水准而存在。如果数字网络中的其他人没有相似水平的隐私，那么任何个人也无法拥有同样的隐私。因此，隐私保护不再只是个人权利问题，也成为公共品提供和社会整体福利增进的命题。

（三）价值基础：公共善与分配正义

对于隐私权的理解，有必要超越狭隘的个人主义视野，突破原子论的权利范式，从公共善和社会正义的高度，在本体论和价值论层面作出重新诠释。

第一，隐私作为社会尊严价值。隐私的价值基础始终存在某种内在矛盾：一方面，隐私的主要价值是促进和保护个人自主；另一方面，个人自主的实现却深度依赖社会，个人自主乃社会塑造的产物。晚近以来，许多学者都开始将隐私视为一种公共善，而不是简单的个人善。尤其是罗伯特·波斯特（Robert Post）区分了数据隐私和尊严隐私概念：数据隐私强调信息控制的抽象需求，将人类想象为数据的自主操纵者，预设差异，对社会意义漠不关心；尊严隐私则着力诠释隐私的社会意涵，强调隐私依托的社群规范与习俗，尤其要求尊重超个人的社会道德结构和公共利益。[63] 在波斯特看来，隐私保护的其实是塑造人类团体生活的“文明规则”[64]，正是在彼此尊重的社会规范中，隐私才得以出现和维持。正是在这一视角下，波斯特从信任和公共善等社群主义价值层面，将隐私视为用来协调与他人日常关系的社会尊严规范，将隐私的价值基础重置于主体间性的社会语境。

第二，隐私作为社会语境价值。隐私不仅保护一般性的社会尊严价值，也促成特定语境目的、目标与价值的实现。[65] 隐私法始终需要处理维护个人自主和为促进社会沟通而传播信息之间的矛盾，两者之间的张力，又往往通过特定的语境和场景展开。因此，对于隐私性质的理解，必须联系相应的社会语境以及与之相关的语境价值和语境期待。换言之，人们的隐私诉求不是抽象的，无法推广到普遍的环境，而是高度依赖语境。在这个意义上，隐私不只保护个人价值，也保护外在于个人的社会语境价值。而当代数字技术之所以具有破坏性，不只是因为它们侵犯了个人隐私，也是因为它们使偏离各种根深蒂固的社会语境价值成为可能。许多新颖的数字技术和商业模式不只侵害个人权利，也违反了传统的隐私语境规范，破坏了社会的语境价值。

---

[62] *See* Frederick Schauer, *Free Speech and the Social Construction of Privacy*, Social research, Vol.68:221, p.221 (2001).

[63] *See* Robert Post, *supra* note 10, 1055-1056.

[64] Robert Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, California Law Review, Vol.77:957, p.968 (1989).

[65] 语境由特征性的活动与实践、功能（或角色）、目标、目的、制度结构、价值和行动规范构成，它们可以通过规则或法律明确表达，或者潜在于惯例、规范、实践以及“常规性”行为之中。*See* Helen Nissenbaum, *Respect for Context as a Benchmark for Privacy Online: What It Is and Isn't*, in Carine Dartiguepeyrou ed., The Futures of Privacy, Foundation Télécom, 2014, p.23-28.

第三，隐私作为社会构成性价值。传统隐私的价值论证注重强调个人主义的维度，未能充分把握隐私更为深刻的社会意涵。而在社会构成性价值的视角下，隐私就不只是针对个人自主的价值，同时作为体现社会整体性建构的价值，嵌入社会规范和社会惯例。正是在这个意义上，保罗·施瓦茨（Paul Schwartz）强调，隐私应作为一种“构成性价值”进行保护，因为它是个人与社会被创造和维护的方式之一。[66] 隐私乃是一种社会关系，是人类互动的结构性要素；隐私在本质上是社会性的，正是通过隐私，才得以建构一整套解释与处理自我和他者关系的社会规范标准。[67] 质言之，隐私议题涉及人类社会的总体存在状态，无法简化为信息采集和数据处理等客观事实，必须结合相应的社会图景和社会理想才能深入理解。正因如此，作为社会构成性价值的隐私，应当由所有社会行动者共享并共同保护。

第四，隐私作为社会分配正义价值。当代隐私法需要处理个人－个人、个人－社会、个人－国家的价值冲突和权益衡量问题。首先，以个人－个人的横向冲突为例，在数字时代背景下，个人的隐私决策不再只是涉己行为，同时也转化为影响他人利益的涉他行为。其次，以个人－社会的横向冲突为例，在个人隐私保护和社会对数据的合理利用以及技术发展、商业创新等目标之间存在张力。最后，以个人－国家的纵向冲突为例，在个人隐私保护和政府获取治理信息等目标之间存在矛盾，即如何平衡个人隐私与国家安全等价值之间的利害关系。处理上述价值冲突都需要立足分配正义层面的价值衡量。申言之，当前的隐私保护无法只考虑个人维度的得失，同时也牵涉极为复杂的个人、社会与国家多元维度的法益分配和价值权衡，因此必须从社会正义的高度、从公平公正的价值维度重新审视隐私保护。

（四）法律概念：隐私权的社会建构性

隐私权的含义并非固定不变，而是具有鲜明的社会建构性特征。技术发展、商业创新与法律博弈的多重因素持续推动着隐私权的概念转变，及时回应并深刻塑造了社会公众的隐私期待。

第一，隐私权是社会建构性的法律概念。首先，现代隐私权有关隐私合理期待的标准，事实上就包含了关于什么是隐私的社会性理解，即认为隐私与特定的社会期待相联系。这就与传统的二元论隐私，即将个人与社会相互割裂的做法相悖。其次，二元论隐私，即将个人（私人）与社会（公共）相互对立的理解，其优点是可以为隐私保护提供确定的判断标准，明晰把握隐私的保护对象。但在数字时代，隐私保护针对的不是处于真空中的个人，个人已经深度嵌入各种社会技术系统和数字制度之中。二元论隐私的简洁性已经难以把握正在发生深刻演变的隐私的特征和性质。最后，隐私概念隐含了社会结构、伦理规范和法律义务的复杂内涵，这些社会因素共同塑造了隐私权的丰富含义。在法律实践中，对于“可识别性”以及“与自然人相关性”等法律概念的解释，其实也

---

[66] *See* Paul Schwartz, *supra* note 7, 834.

[67] *See* Valerie Steeves, *Reclaiming the Social Value of Privacy*, in Ian Kerr et al. eds., Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society, Oxford University Press, 2009, p.196.

都涉及对于什么构成识别可能性以及信息与自然人相关关系的社会理解，最终都牵涉相关的社会期待和社会建构。也是在这种背景下，隐私权正不断演化为知识密集型与社会建构化的法律概念。[68]

第二，个人信息是社会建构性的法律概念。传统隐私法并不承认在个人信息和非个人信息之外，还存在第三种状态。而数字时代的基本事实是，个人信息概念愈益泛化，要求获得保护的个人信息范围愈益扩展，个人信息与非个人信息的边界愈加模糊，也更加具有争议性。首先，信息不仅可以在内容上，也可以在主观目的或客观结果上与个人“相关”，个人信息不再只是“关于”（about）个人的信息，也包括与个人“关联”（relate to）的信息。[69] 任何信息都可能在主观预期影响和客观结果影响的意义上，与个人发生直接或间接的关联。其次，个人信息与非个人信息法律概念的界分本身就是历史的产物，隐私法的早期理论实际上并未将个人信息概念作为基础。[70] 而在数字时代，个人信息不断被处理成最适合商业模式开发的形式，既是自然的又是经过人类加工的。换言之，在数字技术条件下，已经很难再有完全意义上的非个人信息，各类非个人信息都可能通过再识别和去匿名化技术转变为个人信息。伴随新的技术演进，“潜在的个人信息列表将永远不会停止增长，直到包含所有内容”[71]。正因如此，个人信息的保护范围最终取决于法律的建构和解释。

第三，隐私权的救济机制也面临社会化转向。首先，在今天，大多数数字系统不是单个程序员的作品，而是团体或组织协作的产品，其中包括设计师、工程师、程序员、心理学家、图形艺术家、投资经理和营销团队等各种主体，社会技术系统的决策通常是众多行动者合作互动或相互博弈的结果。在这种情况下，确定个人的侵权责任变得越发棘手，复杂的相互耦合的数字系统侵蚀了个人责任的概念。其次，传统的隐私救济需要对侵权因果关系进行个案调查和举证，但数字隐私的侵害形式却表现为零星、高发、弥散化和分布式的特点。在这种背景下，隐私侵权的因果链条难以完整建立，只能在总体上预测隐私侵害的概率，评估隐私风险的相关性。数据的大规模处理对个人可能只以小规模程度形成隐私削减，但即使对个人隐私只造成轻微伤害，社会的综合成本也可能非常高昂。最后，正如前述，个人信息法律概念是历史的产物，与 20 世纪中叶计算机和数据库技术的发展息息相关。因此，如果将特定发展阶段的法律概念本质化，那么就可能因为新技术

---

[68] 当代隐私侵害“不取决于单一确定的原因，而是取决于多种潜在原因，即风险因素”，个人本位的隐私法概念（例如侵权因果关系），正被社会本位的隐私法概念取代（例如风险因素分析）。*See* Gellert Raphaël, *Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative*, International Data Privacy Law, Vol.5:3, p.15 (2015).

[69] 第一，“个人”一词应理解成什么？第二，在什么情况下才算是“个人”事项？某个“个人”事项是否仅仅因为个人声称它是“个人”的，或者存在本质上是个人的事项？ 参见［英］雷蒙德·瓦克斯：《隐私》，谭宇生译，译林出版社 2020 年版，第 35 页。

[70] *See* Daniel Solove & Paul Schwartz, *supra* note 41, 1818-1819.

[71] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, UCLA Law Review, Vol.57:1701, p.1742 (2010).

对于既有隐私保护条件的破坏，从而放弃对于作为保护对象的隐私价值的追求。

四、构建六位一体的隐私权保护体系

数字时代，各类技术、组织、制度与法律之间不仅形成反馈回路，同时也形成共同演化机制。数字社会的高度复杂特征，要求我们超越个人与社会、私人与公共的二元论，深入探索隐私保护的新模式。首先，社会本位的社会不是可视化的单一物质实体，而是立足于不同观察视角建构的框架化机制。不同的社会化视角可以采取动员、组织、建模、规范、整合、激活成员与资源的多元方式，提供隐私社会本位保护的不同模式。其次，社会本位区别于国家本位，国家视角只是隐私社会本位保护模式的方案之一。正是为了避免单一的经济、政治、科学、伦理、技术、法律视角的弊端，笔者尝试搭建一个涵括市场、国家、风险、语境、网络、权利维度的六位一体社会本位保护模式。最后，既从统一社会本位（市场、国家、风险）的角度，也从分化社会本位（语境、网络、权利）的角度，提出构建一套相互竞争、内在制衡、嵌合补足的隐私保护体系。

其一是市场模式。社会本位的一个基本思路，是将社会理解为由市场机制自我整合的契约结构，以此构筑隐私保护的内在动机、自主激励和自发动力机制。面对数字时代形成的复杂的共生网络关系，必须充分利用商业模式作为技术与法律规范演化的力量。实践中，国家的强力监管由于对市场机制不敏感，反而有可能阻碍各种潜在的有利于隐私保护的商业和技术创新。因此，必须为隐私保护设计合理的市场激励机制，通过重塑市场规则，不断提升个人防止隐私侵害和参与数据交易的能力。同时，鉴于数字社会的规模性和复杂性，如果无法充分利用市场与企业的信息收集、处理和监控能力，隐私保护的目标势必难以实现，而这要求“公司自己发展内部控制来识别、评估与降低风险”[72]。有研究者已观察到，不同信息供应链中的组织会对上下游合作伙伴的隐私管理实践产生深刻影响。[73] 当然，由于市场外部性、不完备性与交易成本等问题，单靠市场力量无法保证带来最有效的隐私保护结果。特别是，法律经济学的成本收益分析有可能持续低估分散、累积且难以用货币价值术语描述的隐私伤害，并由此进一步巩固既得利益主体的特权地位。

其二是国家组织－监管模式。社会本位的另一基本思路是强化组织型和监管型国家的作用，让社会在强制整合的意义上，实现一种强制隐私的保护状态。它既可以呈现为克里斯蒂安·法克斯（Christian Fuchs）所设想的社会主义隐私概念，[74] 也可以通过国

---

[72] Kenneth Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, Texas Law Review, Vol.88:669, p.672 (2010).

[73] “大数据行业的系统性参与引发了‘人人都这样做’的伦理问题——实践规范开始在许多公司和供应链中形成。” Kirsten Martin, *Ethical Issues in the Big Data Industry*, Routledge, 2020, p.75.

[74] “社会主义隐私概念将隐私视为一种受支配和剥削团体的集体性权利，以对抗公司的支配。” Christian Fuchs, *Towards an Alternative Concept of Privacy*, Journal of Information, Communication & Ethics in Society, Vol.9:220, p.231 (2011).

家深度介入、引导与监管隐私市场的方式进行。区别于自发的市场机制，国家组织－监管模式可以构筑不同的具有法律责任承担能力的集体资源池，与此同时，它也特别突出了具有控制能力的中心枢纽的角色，尤其是国家在隐私保护中所具有的协调能力。当然，国家组织－监管模式也存在弊端。一方面，硬家长主义的强制隐私对于特定社会成员可能缺乏吸引力；另一方面，存在挫败市场自身隐私保护创新动力的可能。

其三是风险治理模式。市场模式是将社会理解为自发的多中心机制，国家组织－监管模式是为社会创设特定的控制中心，而风险视野的社会本位，则是一种适应当代高度不确定和复杂状态的社会表征化机制。因为在数字时代，只有通过特定的建模与表征，社会才能充分理解和处置各类系统性风险。质言之，风险是通过统计学与概率论评估的社会伤害。作为一种社会治理技术，它将不确定的未来危险转化为特定的量化风险，由此，就可以引入来自经济学（成本收益分析）和科学（风险评估技术）的各种风险管理工具。在这个意义上，风险摒弃了基于个人本位的因果责任法律概念，通过消除寻找个别因果关系的需要，风险治理试图在社会本位的层面进行社会修复。风险源于多种不同因素的相互作用，其表现形式因环境而异。正因如此，社会本位的风险治理迥异于传统隐私的救济方式。基于风险的隐私治理主要针对当代数字系统的互联性特征，这些互联系统无法作为可识别的行动单元，因此难以准确界定法律责任的比例。这就需要通过风险社会化的方式应对，无论是通过强制性保险（国家组织）实现完全的社会化，还是通过从互联系统中获得经济利益的行业部门实现部分的社会化，其核心逻辑都是“建立一个充足的资金池来弥补损失并分散风险”[75]。当然，风险治理模式同样面临困境。首先，是风险治理立足的经济学与科学工具的局限性，这些工具的“假设、标准、认知和方法承诺是什么，它的限制是什么，还有哪些其他类型的知识是相关的”[76]？其次，风险社会化可能对数字互联系统的开发者提供错误的激励，鼓励其粗心大意的行为，并由此大大限制侵权法的控制功能。再次，如何避免为管理风险而开发的技术系统反过来成为新的风险来源？最后，并非所有与隐私侵害有关的风险因素都可以建模和量化。

其四是语境－场景－系统模式。市场、组织和风险模式都在一种整体性的意义上把握社会，而语境模式并不寻求涵盖整个社会的综合隐私解决方案，它试图在适当规模的社会领域处理隐私问题，通过特定的语境锚点来建立相应的隐私规制框架。首先，语境模式预设不同社会领域都受内部相应的信息规范支配，并不存在可以普遍适用于所有领域的隐私规范。在这种理念支持下，相应社会语境的信息规范就可以成为相关隐私争议的仲裁标准，无论是市场、医疗、教育、政治、科学、家庭，都可以根据其特定的语境目标、目的和价值，为隐私保护提供具体的指引。其次，隐私保护在语境模式下可以呈现为领域敏感与功能分化的状态，这可以防止特定社会系统对于隐私解释的垄断，防止过度统

---

[75] Anna Beckers & Gunther Teubner, *Three Liability Regimes for Artificial Intelligence:Algorithmic Actants, Hybrids, Crowds*, Hart Publishing, 2022, p.162.

[76] Brian Wynne, *Uncertainty and Environmental Learning—Reconceiving Science and Policy in the Preventive Paradigm*, Global Environmental Change, Vol.2:111, p.118 (1992).

一的社会化模式对个人隐私权利的挤压，尤其是限制经济和政治部门对于其他社会领域隐私规范的支配。但是，语境模式也存在保守主义的偏见。数字时代背景下，语境往往处于动态演化的状态，并不存在固定不变的信息规范。传统的社会语境正在剧烈重组，语境边界愈加模糊，某种语境的信息规范不断渗透与蔓延到其他语境，不同的语境价值产生混合、重叠与冲突，这导致“在社会网络世界中描述语境特别困难”[77]。尤其是各类数据信息会不断经历去语境化和再语境化，这也使得语境模式无法为此提供准确定位的法律解释工具。质言之，传统语境具有独立性、自主性和完整性的特点，而新的社会语境则具有虚拟性、交叉性与跨语境特征。在这种背景下，隐私保护就要求从语境模式进一步迈向系统论和场景论视角，趋向一种更动态化的规制模式。

其五是网络－社会数字制度模式。网络理论和语境理论同样是从社会分化的视角来定义社会本位保护模式。首先，与去中心的市场和中心化的组织监管不同，网络是动态演化的社会机制，它立足于市场的多边合同与组织的等级科层之间来理解社会的结构，因此同时具备了市场取向的自发性和组织取向的强制性。其次，网络模式视角下的社会，是一个由不同中心枢纽组织和围绕枢纽的大量多边合约节点组成的不对称网络，这些连接形成了一种社会共同事业的纽带。在今天，各种建立与运行信任网络的社会机制为不同主体搭建系统规则，多方共享架构与各类标准协议对可扩展网络中的所有参与者产生了约束性义务和责任期待。[78] 由此，网络模式下可以探索隐私保护的分布式责任概念：网络中的每个实体都可能对归属于该网络的其他实体承担连带责任。因为在新的数字网络中，无论是将法律责任归于个人、制造商、平台守门人或算法节点都无法令人信服，法律责任呈现为结构性分散的状态。这需要网络理论根据不同节点的强度和影响，根据相应的网络份额、利益与控制能力，对法律责任进行比例化的分配。进言之，网络模式的归责机制更有助于隐私受害者直接向网络参与者提起赔偿请求，免于证明个人过错的负担，“外部责任引导最终以追偿行动的形式与内部责任分配相辅相成”[79]。最后，与网络概念相呼应，制度概念同样既不同于市场也不同于组织。作为同时具有认知性和规范性特征的社会期望复合体，制度在当代正进一步演化为社会数字制度。作为不同技术和社会系统之间的结构耦合机制，社会数字制度与社会网络共同演化，将成为隐私保护的新型单元。

其六是基于权利的公共商谈模式。基于主观权利的侵权法作为一种学习和反馈机制具有独特优势。[80] 私人权利通过诉讼机制，可以从外部激扰监管矩阵，最终影响为隐私

---

[77] Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, Yale Journal of Law & Technology, Vol.16:1, p.25 (2013).

[78] 系统规则在信用卡语境中称为“操作规则”，在身份联合语境中称为“信任框架”，在供应价值链语境中称为“贸易伙伴协议”。此外，系统规则的设计允许参与者广泛分布在异构的商业所有权边界、法律治理结构和技术安全领域。*See* Daniel Greenwood et al., *The New Deal on Data: A Framework for Institutional Controls*, in Julia Lane et al. eds., *supra* note 21, 7.

[79] Anna Beckers & Gunther Teubner, *supra* note 75, 133-139.

[80] *See* Mary Lyndon, *Tort Law and Technology*, The Yale Journal on Regulation, Vol.12:137, p.176 (1995).

保护创造环境的商业模式。但问题在于,新的数字环境下,个人往往沦为各种临时算法群组的被动成员,即使被授予救济请求权,也由于缺乏能动性与资源,往往难以采取有效行动保护自己的隐私利益。然而,作为权利的隐私不只是个人自决和同意权,也不只是私人自主的概念,它还可以成为社会契约论意义上的公共自主概念。因此,隐私权利的实现,不能单向取决于私人自主或国家司法,而需要同步激活公共自主和商谈对话过程。只有在公共商谈的意义上激活数字公共领域,才有可能生成、反思并修正持续演化的隐私规范。正是在这个意义上,隐私乃是主体间的商谈性权利,它“等同于信任”,“与信任相关”,是“与信任相关的核心价值”[81]。质言之,隐私的公共自主和私人自主并不矛盾,相反,公共自主与私人自主互为前提和条件,从而构成隐私权利的一体两面。

五、结　语

我国《个人信息保护法》于2021年颁布并实施,昭示了立法者对于数字隐私保护的重要决断。立法者从领域法的高度,面对高度复杂的数字时代,以人格尊严为基本价值设定,从多元治理的视角,对个人信息保护的制度结构进行了体系性的谋划。

数字时代背景下,隐私保护涉及的法律主体和法律关系愈益复杂,保护对象所处的领域已逐渐溢出平等民事主体的范畴,因此需要避免采用单一保护模式,正视数字时代隐私侵害责任的复合性质,迈向融贯公私法的问题导向型保护模式。必须强调,隐私的社会本位保护并不妨碍在法益归属上对个人获益作出基本判断,亦不违反民事法律的基本原理,更不构成否认私权保障的立场。发展领域法,并不意味着部门法边界的消除,而恰恰需要部门法学研究的精进。不同部门法需要在新的观察模式下作出回应,吸收来自社会变迁的刺激。伴随隐私生产的社会建构性甚至网络化再生产,基于民法的个人请求权当然不会消失,而且应当发挥更重要的作用,但是请求的范围、内容、程序、举证责任等都会发生相应变化。[82]

隐私作为数字时代的基本权利,既暴露了传统权利话语的不足,也为发展更好适应数字时代权利保护的新形式指明了方向。隐私权具有演化、动态的特质,其渐增性和继承性特征是对社会变迁的回应。正是在社会演进中,隐私权得以更新与发展,逐渐落实为具有更丰富内涵的权利形态。[83] 隐私保护的新模式不以替代旧模式为前提,个人本位与社会本位不是互相取代和排斥,而是相互依赖与交叠的关系。在法律实践中,新旧模式可以长期共存,互动激扰,依据社会发展和历史时势的变化,借由立法者、司法者与法律研究者的创造性工作,理性审慎地调整相应的组合比例。

考虑到我国隐私保护制度尚不完善、行政监管机制尚不健全等背景,民法保护具有

---

[81] *See* Kenneth Bamberger & Deirdre Mulligan, *Privacy on the Books and on the Ground*, Stanford Law Review, Vol.63:247, p.270 (2011).

[82] 参见程啸:《论〈民法典〉与〈个人信息保护法〉的关系》,载《法律科学》2022年第3期,第21-30页。

[83] 参见余成峰:《信息隐私权的宪法时刻:规范基础与体系重构》,载《中外法学》2021年第1期,第52页。

重要的价值导向和实践指引功能。《民法典》立足人格尊严之法律价值，首次从民事基本法的高度确认隐私和个人信息受法律保护。在当前阶段，应进一步增强隐私权的民法保护力度。而在法理基础上，可以探索个人本位保护与社会本位保护的融合，追求体用兼备、并行不悖的理想格局。伴随数字经济发展，根据新的时代需要，对隐私权保护体系进行持续的增量建设。综合不同法律技术和监管工具，通过兼容并包、相互涵纳、内在制衡、协调统合的制度构建，最终形成商业市场、组织监管、风险治理、语境场景、网络制度、公共商谈模式在内的系统化隐私法律保护生态。

Abstract: Modern privacy law is based on the three theoretical presuppositions of individualism, the dichotomy between the individual and society, and the concept of personal information, which converge into two core paradigms of control privacy and access privacy, shaping the privacy tradition of individualism. In the context of the digital age, with changes in actors, communication modes, and information types, as well as the macro-structural transformation of platformization and scale, the individual-based tradition of privacy is facing difficulties. From the four aspects of social structure, social function, value basis and legal concept, individual-based privacy protection needs to be further combined with social-based protection. Based on China's national conditions, we should actively explore the integration of individual-based protection and social-based protection, and integrate different legal techniques and regulatory tools, and through the system construction of mutual inclusion, internal checks and balances, and coordination and integration, a systematic legal protection ecology including commercial markets, organizational supervision, risk governance, contextual scenarios, network institutions, and public discourse models will eventually be formed.

（责任编辑：强梅梅）