中外法学 Peking University Law Journal
Vol.33, No.1(2021)pp.32－56

信息隐私权的宪法时刻
规范基础与体系重构

余成峰*

摘　要　信息隐私权的传统规范基础以个人为本位，以私人和公共为二分法，围绕空间、事物与主体维度，形成五种理论解释和六项概念核心。隐私的洛克范式与康德范式，晚近以来汇流为控制范式，成为当代信息隐私保护的核心原则。智能社会，特别是大数据技术，瓦解了控制范式的技术假设，进而对信息隐私权的规范基础形成全面冲击和挑战。技术巨变重构了社会图景，在空间、时间与社会维度引发隐私保护的深刻困境。需要从信息论和社会理论视角重新理解隐私，重构信息隐私权的规范基础：从个人本位转向社会本位；从控制范式转向信任范式；从独占维度转向沟通维度；从二元对峙转向一体多元；从权利视角转向权力视角；从概念独断转向语用商谈。在宪法时刻的时间意识下，为我国信息隐私法的未来发展寻找新的体系框架。

关 键 词　信息隐私权　规范基础　体系重构　大数据技术　宪法时刻

随着新型信息技术的迅猛发展，隐私正受到全方位挑战，论者甚至发出“零隐私社会”“隐私的死亡”这些警告。在新技术条件下，当“可隐性”逐步瓦解，隐私的成立和维护变得岌岌可危。事实上，在智能社会，信息隐私权乃是发展“第四代人权”与“数字人权”至关重要的环节。〔1〕迫

* 北京航空航天大学高研院/法学院副教授。本文系国家社科基金一般项目“第三波法律全球化范式变迁研究”（项目编号：20BFX008）的阶段性成果。

〔1〕 参见马长山：“智慧社会背景下的‘第四代人权’及其保障”，《中国法学》2019 年第 5 期，第 5－24 页。

切需要对信息隐私权的规范基础展开深入讨论。〔2〕近代隐私是印刷术时代的技术赋能。〔3〕换言之，隐私并非个人的天然权益，它深刻取决于信息和通讯的基础设施。一旦旧的技术架构被数字时代大量的互联互通与计算主义转向改变，隐私的规范基础也就必须重构。这要求我们从新的社会和技术视野出发，为信息隐私权的未来发展提出新的指导原则与体系框架。

全文论证脉络如下：第一部分对信息隐私权的传统规范基础进行了概括；第二部分阐述新技术变革对隐私规范基础的冲击与挑战；第三部分为隐私权重构提出新的原则方向；最后，在宪法时刻的时间意识下，为我国信息隐私法的未来发展寻找新的体系框架。

一、传统与当代：信息隐私权的规范基础

（一）信息隐私权的传统规范基础

自1890年沃伦和布兰代斯的名篇《隐私权》发表以来，〔4〕信息隐私权的规范基础几经流变，可以概括为一个本位、两种范式、三个维度、四组二分法、五种理论与六项概念。

首先，信息隐私权的规范基础以个人为本位。特定个人拥有特定隐私以及遭受特定侵害的可能，这种意象一直主宰隐私权的解释与实践。隐私被定位为一种与世界隔离和对抗的个人权利概念，它乃是个体“保持独处的权利”（right to be let alone），与“围墙”“财产边界”“共有体验的切断”这些隐喻相联系。〔5〕其要义是“给个人制造一个特定的私人地带”。〔6〕学者认为，现代隐私产生于印刷媒体的发明，伴随印刷媒体制造的公共、匿名与非个人领域，也连带产生了私人领域，隐私正是保护这一个人自主性不被印刷媒体带来的公共性吞没。〔7〕于此，沃伦和布兰代斯将隐私定义为“个体”的“独处权”，与此呼应的普通法隐私侵权，也将目标牢固锁

〔2〕毋庸置疑，个人信息保护已突破传统的隐私权范畴，这是目前我国学界与实务界区分使用隐私权和个人信息保护概念的原因。但是，隐私权拥有深厚的历史传统，是演化性、历时性、包容性的概念，能为个人信息保护提供规范与价值层面的支撑。事实上，在信息时代，隐私主要就表现为信息隐私的形式。因此，笔者不赞成将这两个概念割裂处理，主张学理层面可在“大隐私”范畴下统合使用“信息隐私权”概念，它区别于民法上的“隐私权”，也区别于狭义的“信息隐私”（information privacy）概念，进一步分析可见本文结语部分。有关隐私权和个人信息保护，我国学者已展开广泛讨论，例见张新宝：“从隐私到个人信息：利益再衡量的理论与制度安排”，《中国法学》2015年第3期，第38－59页；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”，《现代法学》2013年第4期，第62－72页；丁晓东：“个人信息权利的反思与重塑——论个人信息保护的适用前提与法益基础”，《中外法学》2020年第2期，第339－356页。

〔3〕See Felix Stalder, “The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy”, *Sociological Research Online*, Vol.7, No.2, 2002, pp.1－15.

〔4〕See Warren and Brandeis, “The Right to Privacy”, *Harvard Law Review*, Vol.4, No.5, 1890, pp.193－220.

〔5〕See Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age*, Cambridge: Cambridge University Press, 2018, p.13.

〔6〕Ibid, p.17.

〔7〕See Mireille Hildebrandt and Katja de Vries (eds.), *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*, New York: Routledge, 2013, p.136.

定在保护个人。〔8〕正是通过这些法律保护，一个称为“隐私权”的个人领域产生了。由此，信息隐私权的规范基础是个人本位的权利，指向一切可被识别到个人的信息。〔9〕在此理解下，隐私侵权是特定的错误行为人做出特定的行为，由此给特定个体带来的特定伤害。正如美国《第二次侵权法重述》所规定：隐私是个人权利，针对的是个人隐私被侵入的情况。〔10〕而在普通法之外，美国隐私的宪法和特别立法保护，其规范定位也都落在个人之上。〔11〕同样，欧洲理事会早在 1970 年代就将数据保护法的对象界定为自然人的个人信息，1995 年的《数据保护指令》(DPD)和最新的《通用数据保护条例》(GDPR)也都无例外地聚焦于数据主体的权利，隐私保护始终围绕个人的已识别或可识别信息。〔12〕综上，信息隐私权的规范基础采取严格的方法论个人主义，以个人为中心和本位，通过个体化策略进行隐私权的解释与应用。

其次，信息隐私权的规范基础扎根于两种哲学范式，即洛克传统和康德传统。洛克传统强调隐私权的消极面向，主张私人生活摆脱公共之眼的注视；而康德传统注重隐私权人格自主的维度。美国隐私法主要受洛克传统影响，隐私权首先是一种消极权利，强调“隔离”(seclusion)“独处”与“秘密”，主要落实于侵权法；欧洲隐私法主要受康德传统影响，隐私被定位为“人格权”和“信息自决权”，强调自我表达、自主发展身份与认同，晚近以来，更是上升为宪法性的“基本权利”。〔13〕洛克范式下，隐私是“自我所有权”(self-ownership)的客体，隐私所有者以财产形式占有隐私，并排除他人侵犯。〔14〕正因如此，美国普通法尤其强调隐私的财产特征，特别是“私人空间的神圣不可侵犯”。〔15〕“完美的隐私是完全无法被他人接近。”〔16〕而在康德范式下，隐私联系于人格的自由意志，“隐私是人作为人的完整性”。〔17〕隐私保护个体的自治、独立与自决，在德国更是发展为事关人类尊严的宪法权利。〔18〕如果说，洛克传统下隐私和财产

〔8〕 Warren et al., supra note 4, p.195; William Prosser, “Privacy”, *California Law Review*, Vol. 48, 1960, pp.383－423.

〔9〕 See Bart van der Sloot, *Privacy as Virtue: Moving Beyond the Individual in the Age of Big Data*, Amsterdam: Intersentia, 2017, pp.4,11.

〔10〕 Quoted from Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age*, New York: NYU Press, 2004, p.94.

〔11〕 See Helen Nissenbaum, “Privacy as Contextual Integrity”, *Washington Law Review*, Vol.79, No. 1, 2004, p.129.

〔12〕 See Taylor, Floridi and Sloot (eds.), *Group Privacy: New Challenges of Data Technologies*, Dordrecht: Springer, 2016, p.5.

〔13〕 Sloot, supra note 9, pp.13－14.

〔14〕 See Janice Richardson, *Law and the Philosophy of Privacy*, New York: Routledge, 2016, p.15.

〔15〕 Nissenbaum, supra note 11, p.129.

〔16〕 Ruth Gavision, “Privacy and the Limits of the Law”, *Yale Law Journal*, Vol.89, No.3, 1980, p. 428.

〔17〕 Charles Fried, “Privacy”, *Yale Law Journal*, Vol.77, 1968, p.477.

〔18〕 See Mireille Hildebrandt, *Smart Technologies and the End(s) of Law*, Cheltenham: Edward Elgar Publishing, 2015, p.79.

概念关联，康德传统则突出隐私的人格尊严维度。〔19〕综上，洛克范式强调隐私作为私域与公域的分离和对抗，康德传统则注重人格与身份的自由发展。晚近以来，两大范式合流，共同构成信息隐私权的哲学基础，即从消极和积极两方面，将隐私重构为个人对自我信息边界的控制，并落实于当代隐私法普遍应用的告知—同意原则（notice-and-consent framework）。〔20〕

第三，信息隐私权的规范基础围绕空间（space）、事物（thing）与主体（ego）三个维度展开。首先，隐私是公共性不能进入和控制的“空间领域”。〔21〕隐私是在空间上占据特定范围、获得特有领地、拥有特殊边界的概念。其空间意象与墙壁、隔断、幕布、窗帘等联系，从而确立物理性或心理性的隔离空间。在此理解下，隐私侵犯即是对隐私空间（where）的侵犯，辨别侵害发生的依据，即是对此类空间的指认和确认。其次，隐私是一种特殊的“事物”（what），这一事物（thing）具有亲密性（intimacy）、秘密性（secrecy）或敏感性（sensitive）。隐私确权的关键，即在事物维度判别其“本质”，不同隐私理论因此做出各不相同的界定。〔22〕其三，隐私的主体维度是内向与孤独的自我，由自我主导隐私边界，捍卫并抵挡外部的侵入。换言之，在这种理解下，隐私主体是理性、自主的行动者，有能力掌控自己的隐私命运。〔23〕综上，信息隐私权乃是特定主体在特定空间占有特定隐私事物的三维意象，由此创造了一个在空间上隔离、在社会关系上孤立的原子化形象。

第四，信息隐私权的规范基础倚赖于四组私人/公共二分法的建构。这四组二分法又是依据上述三维视角建立。在空间维度，建立了私人空间（领域）和公共空间（领域）的二分；在事物维度，创立了个人信息（数据）与公共信息（数据）的二分；在主体维度，建构了私人/公共、主体/客体两组二分法。这四组二分法成为隐私权理论和实践的重要工具。首先，在空间维度，隐私被定位于私人领域，而对私人领域的确定，则又反身性地取决于私人与公共的划分，易言之，隐私即在于假设在空间上“有一个界限将私人和公共区分开来”。〔24〕其二，“公共”概念具有高度弹性，既可以指公共物理空间，也可以指不特定他者的注视，既可以指国家主权，也可能指代公共利益。这些不同定位都会深刻影响隐私范围的确定与评价。其三，相比于抽象的人格，“空间”概念更具法律操作性，以确保建立稳定的隐私期待。沃伦和布兰代斯也因此强调保护隐私即保护私人空间。〔25〕实践中，私人/公共空间二分法不断灵活限缩或扩大对隐私的保

〔19〕 See James Q. Whitman, “The Two Western Cultures of Privacy: Dignity versus Liberty”, *Yale Law Journal*, Vol.113, 2003, pp.1176, 1193, 1212.

〔20〕 Richardson, supra note 14, pp.66－71.

〔21〕 See Milton Konvitz, “Privacy and the Law: A Philosophical Prelude”, *Law and Contemporary Problems*, Vol.31, No.2, 1966, pp.272－280.

〔22〕 例如，隐私法学者索罗夫就强调“作为亲密关系的隐私”（privacy as intimacy），论证这一概念如何支配美国的联邦隐私立法与最高法院的司法实践：亲密性是隐私的事物“本质”，因此，信息一旦公开，也就不再成其为隐私。Waldman, supra note 5, pp.20－21.

〔23〕 See Neil Richards and Woodrow Hartzog, “Taking Trust Seriously in Privacy Law”, *Stanford Technology Law Review*, Vol.19, No.1, 2015, p.437.

〔24〕 Judith DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Ithaca: Cornell University Press, 1997, p.10.

〔25〕 Warren et al., supra note 4, p.90.

护：即使是私人信息，一旦进入公共空间，就无法作为“隐私”保护；即便发生在公共空间的对话，一旦在法律上被界定为“私人领域”，也应作为“隐私”对待。〔26〕 其四，在事物维度，个人/公共信息二分法也成为普遍应用的法律工具。隐私乃是“防止访问私人信息的一种保护措施”，〔27〕这些信息有关“私人生活、习性、行为以及人际关系”。〔28〕 普通法隐私侵权的典型类型，即“公开揭露令原告难堪的私人事实”。〔29〕 司法实践中，正是通过区分个人信息与公共信息，隐私的保护范围不断得到确定和调整。〔30〕 最后，在主体维度，隐私法预设了私人与公共之间的防御性关系，隐私乃是个人和公共之间的一道保护屏障。〔31〕 综上，四组二分法对信息隐私权的规范基础在三个维度进行了再区分，进而将隐私界定为居于私人空间的主体占有私人性信息客体并以此对抗公共性的概念。私人/公共二分法成为隐私法领域最具操作性的法律工具箱，四组二分法以“反身性”(reflexive)和“再进入”(re-entry)方式形成复杂的法律组合关系，不断推动隐私理论的演化：一方面确立隐私的定义与范围，另一方面持续调整隐私在规范行为和政策上的效果。

第五，围绕信息隐私权的规范基础形成五种理论解释，即化约主义、所有权、人格、功利主义和权利理论。化约主义认为隐私的价值不在自身，而在于由隐私侵犯所带来的其他道德价值的受损。“隐私是一种工具善，重点则是保护其他目的善(例如尊严、自由与安全)。”〔32〕所有权解释则是洛克传统的延伸，隐私作为“自我所有权”，乃是排他性财产权，是“对整个信息生

〔26〕 美国宪法对垃圾隐私问题，就采用了空间二分法，而不是信息二分法理论。即，虽然垃圾是“私人信息”，但一旦被丢弃到“公共空间”，就不再作为“隐私”保护。See California v. Greenwood, 486 U.S. 35 (1988). 而在 Katz v. United States 案中，正是基于“私人/公共”二分法，最高法院把电话通话界定为宪法保护的“私人领域”(private zone)，宣布 FBI 对电话亭的监听行为违宪。只是，对何谓“私人空间”的解释，在不同时代、社会和文化，会持续改变。例如在美国，1928 年的 Olmstead v. United States 案，美国最高法院宣布窃听行为并不构成对私人空间的侵犯。而到 1967 年的 Kazt v. United States 案推翻了这一判决，认定窃听私人电话构成对私人空间不可接受的侵入。See Olmstead v. United States, 277 U.S. 438 (1928), overruled by Katz v. United States, 389 U.S. 347 (1967).

〔27〕 Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford: Stanford University Press, 2009, p.91.

〔28〕 Warren et al., supra note 4, p.216.

〔29〕 Prosser, supra note 8, p.389.

〔30〕 比如，美国《家庭教育权和隐私权法案》就将学生的记录从“公共信息”改为“私人信息”，在没有学生及其家长明确同意的情况下，禁止对外披露诸如“表现”以及“教师评价”等学生信息。1988 年的《录像带隐私保护法》则把录像带租借记录从“公共信息”改为“私人信息”。美国《爱国者法案》赋予政府机构更大的权力，可以介入到以前被界定为“私人”的众多领域，包括银行和电话记录，甚至是图书馆出借记录。还包括对个人社交网站信息的“私人”或“公共”属性的争论。Nissenbaum, supra note 27, pp.100－102.

〔31〕 美国的隐私保护也通过不同的宪法修正案实现(第 1、3、4、5、9、14 修正案)。主要都是针对政府机构(基于行政和统计目的的电脑数据库)。1974 年的《隐私法案》也是针对联邦机构对个人信息收集、使用和传输的限制，并不包含对私人机构的规制。时至今日，隐私保护仍主要针对政府行动者。Nissenbaum, supra note 27, pp.92－94.

〔32〕 Massimo Durante, *Ethics, Law and the Politics of Information: A Guide to the Philosophy of Luciano Floridi*, Dordrecht: Springer, 2017, p.129.

命周期的控制权”。〔33〕人格理论是康德传统的阐发，隐私赋予人格与身份发展的能力，隐私权是人格在“受侵犯时可以确实寻求保护的法律工具”。〔34〕功利主义则认为隐私首先是一种利益，它不关注隐私的价值本体或权利属性，而着眼对隐私伤害的救济，在事后评估隐私的事实损害。这一思路集中体现于微软公司牵头制定的《21世纪数据保护原则》报告。〔35〕权利理论则认为隐私是实证性法律权利，在美国，隐私既是普通法权利，也是宪法与特别法权利；在欧盟国家，隐私既是民法权利，也是基本权利和国际人权。以上五种解释，除人格理论，都未着力为信息隐私权提供自主的价值论证：化约主义将隐私视为工具善；所有权理论将隐私进行财产定位；功利主义只在事后对隐私进行伤害成本计算；权利理论坚持法律实证立场。〔36〕综上，隐私理论五花八门，但缺乏清晰的哲学论证。人格理论尽管为隐私权提供了价值论证，但人格本身也是有待进一步诠释的抽象概念。

最后，信息隐私权的规范基础可以概括为六项概念核心：即独处、秘密、人格、接近、亲密和控制。其一，布兰代斯、沃伦及隐私法权威学者普罗瑟都将隐私界定为排除他人进入的“独处权”，普通法隐私侵权第一项即针对“侵扰他人的幽居独处或私人事务”。〔37〕隐私乃是“孤独”(solitude)，独处范围既包括身体，也包括作为身体延伸的家庭与房屋。进入独处的私人领域，必须经由同意和允许。〔38〕其次，传统隐私法强调“秘密范式”，即只有“秘密”(secrecy)才是真正“私人”的。〔39〕隐私是对他人隐藏特定的事实，一旦事实公开，就不再作为“秘密”信息，就不再具有“隐私的合理期待”。〔40〕其三，隐私的概念核心也联系于人格。隐私是“保护自由、道德个性、以及丰富和至关重要的内在生活的手段”。〔41〕其四，隐私被理解为他人通过信息、注意力和亲近度来“接近”(access)的程度，隐私是根据对主体的接近(访问)程度来衡量的状

〔33〕 Luciano Floridi, *The Ethics of Information*, Oxford: Oxford University Press, 2013, p.241.在普通法中，隐私利益就被限定在排他的财产界限范围内。Waldman, supra note 5, p.72.

〔34〕 Serge Gutwirth and Mireille Hildebrandt, *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Dordrecht: Springer, 2008, p.318. 人格理论主要盛行于欧洲，但美国最高法院也已在实质正当程序的系列判决中确立隐私权的自由人格理论。Waldman, supra note 5, p.28.

〔35〕 Hildebrandt, supra note 18, pp.201－202.

〔36〕 有关隐私的人格理论，see Jeffrey H. Reiman, “Privacy, Intimacy, and Personhood”, *Philosophy & Public Affairs*, Vol.6, No.1, 1976, pp.26－44. 有关隐私的工具价值和内在价值的讨论，see Charles Fried, *An Anatomy of Values*, Cambridge: Harvard University Press, 1970.

〔37〕 Prosser, supra note 8, p.389.

〔38〕 Nissenbaum, supra note 27, p.96.

〔39〕 Waldman, supra note 5, p.72.

〔40〕 See Daniel Solove, *Understanding Privacy*, Cambridge: Harvard University Press, 2008, p.22.

〔41〕 J. H. Reiman, “Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future”, *Santa Clara Computer and High Technology Law Journal*, Vol.11, No.1, 1995, p.42.“盗用图利”隐私侵权，即用来禁止以商业目的使用人格形象或肖像。Prosser, supra note 8, p.406.

态(条件)。〔42〕隐私即"抵御他者未经允许而接近的能力"。〔43〕其五,隐私也被定位于亲密(intimacy),即某人的亲密关系及相关生活面向。易言之,隐私是一种选择性分享信息的社会能力,它"不仅决定自己与他人的亲密程度,还决定他们关系的性质"。〔44〕其六,晚近以来,隐私的概念核心逐渐统一于"控制"(control),隐私"不仅仅是在别人脑海中缺乏关于我们的信息,也是对我们自身信息的控制"。〔45〕"只有当人们拥有控制自身信息的权利,他才能最大程度地满足自己的隐私偏好。"〔46〕美国最高法院认定,隐私乃是"对个人信息的控制";〔47〕而影响深远的公平信息实践原则(FIPs),其要义也在于为个体设置信息流动的选择权和控制权。〔48〕综上,六项概念也是根据空间、事物与主体维度形成的意象群:独处和接近是空间概念;秘密与亲密是事物概念;人格和控制则是主体概念。从概念演化的视角,接近、亲密与控制分别是对独处、秘密和人格概念的发展,其内在逻辑是增加了隐私的社会视角,突破了传统隐私的孤岛理论,为隐私纳入了能动的社会维度。

(二)信息隐私权的当代范式:作为控制的隐私

从以上梳理可以发现,信息隐私权是具有高度弹性的概念,其规范基础具有多义性。隐私是权利、利益、价值、偏好或仅仅只是一种存在状态?隐私是描述性概念、规范性概念还是法律性概念,或者三者兼有?同时,上述考察也揭示,当代信息隐私权主要落实于两个相对独立的法律框架:其一是基于洛克范式的隐私侵权法,它提供了实体保护原则:例如处理个人数据过程中不能制造伤害;其二是基于康德范式的公平信息实践原则(包括欧盟的个人数据保护原则),它提供了程序保护框架:例如在数据收集、处理和使用过程中,个体享有知情权以及对于相关实践的选择权与同意权。〔49〕洛克范式的伤害原则主要落实于侵权法,康德范式的自主原则主要体现于各类个人信息和数据保护法,两种范式从消极/积极、实体/程序、私法/公法等面向共同构成当代信息隐私权的保护框架。〔50〕

事实上,信息隐私权的规范基础一直伴随信息技术变革而相应调整,隐私概念的演化深刻对应于不同时期的技术发展。〔51〕19 世纪晚期的隐私概念主要针对照相术和大众媒体,核心

〔42〕 See R.Gavison, "Privacy and the Limits of Law", *Yale Law Journal*, Vol.89, No.3, 1980, pp.421－471.

〔43〕 Solove, supra note 40, p.12.

〔44〕 Nissenbaum, supra note 27, p.85.

〔45〕 Charles Fried, "Privacy: A Moral Analysis", *Yale Law Journal*, Vol.77, 1968, p.482.

〔46〕 Nissenbaum, supra note 27, p.72.

〔47〕 Solove, supra note 40, pp.24－25.

〔48〕 参见丁晓东:"论个人信息法律保护的思想渊源与基本原理——基于'公平信息实践'的分析",《现代法学》2019 年第 3 期,第 96－110 页。

〔49〕 有关伤害原则,Sloot, supra note 9, p.103;有关控制原则,see Daniel Solove, "Introduction: Privacy Self-Management and the Consent Dilemma", *Harvard Law Review*, Vol.126, 2012, pp.1880－1903.

〔50〕 Richards et al., supra note 23, p.436.

〔51〕 See Lisa Austin, "Privacy and the Question of Technology", *Law and Philosophy*, Vol.22, No.2, 2003, pp.119－166; Agre and Rotenberg (eds.), *Technology and Privacy: The New Landscape*, Cambridge: MIT Press, 1997.

是防止“侵入”(物理空间的接近);二战之后的隐私概念则主要应对电子数据库技术,解决个人信息自主保护的问题;而在进入新世纪之后,互联网崛起,隐私概念则开始面对信息流动和信息保护的两难问题。〔52〕在新的技术背景下,信息隐私权已开始从原子化、孤立化、隔离化的“独处”与“秘密”概念,不断转向回应信息连带关系的“接近”和“亲密”概念,隐私意象逐渐从“作为隔离的隐私”转向“作为控制的隐私”。一方面,康德范式逐步取代洛克范式,成为信息隐私权的哲学基础;〔53〕另一方面,康德范式的自主原则,又与洛克范式的财产理论形成结合,进而构成新自由主义的隐私控制理论:即将隐私理解为个人信息处分的经济选择行为。〔54〕在这种认知下,告知—同意原则成为具有经济性质的理性选择,“即将个体视为将隐私作为商品经营的企业所有者”。〔55〕

申言之,信息隐私权的规范基础虽几经蜕变,但仍然以个人为中心,以空间、事物和自我为本体论与认识论哲学框架。无论是告知—同意原则、被遗忘权或数据携带权,都仍然“定位于一种个人本位的隐私权概念”。〔56〕尽管信息沟通和数据流动不断转向网络性、连接性与即时性关系,但认知这些信息关系的法律工具,却仍然主要围绕各种私人/公共二分法,定位在主体化、静态化、空间化和排他性的控制框架中处理。这引发了一系列隐私保护的悖论现象:信息与数据流动的社会性和动态性越强,反而强化并巩固了个人本位的隐私控制理论;在表达上越是强调人格理论作为信息隐私权的价值基础,在实践中却越是倾向对隐私进行财产化与合同化理解;〔57〕越是在本体上捍卫“私的隐私”(privacy as private),在结果上就越是无法保护“公的隐私”(privacy as public);〔58〕越是坚持隐私主体的自主权,就越是可能使其主动放弃对于信息的控制权。〔59〕综上所述,信息隐私权的规范基础依旧囿于个体占据私人空间、控制个人信息,进而维护自主人格的传统。新技术发展非但未能改变这一传统,反而进一步强化了“作为控制的隐私”这一意识形态。

---

〔52〕 See Herman Tavani, “Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy”, *Metaphilosophy*, Vol.38, No.1, 2007, pp.6－7.

〔53〕 在康德视角下,隐私伤害不需要首先确立私人空间及其被侵入的发生,也不需要考察被侵入的信息是否属于私密或秘密。相反,只要无形的监控和黑箱性的数据处理活动存在,它们就构成对作为积极的人格构建的隐私权的侵害。Waldman, supra note 5, p.27.

〔54〕 Richardson, supra note 14, p.69.

〔55〕 Richardson, supra note 14, p.71.

〔56〕 Sloot, supra note 9, p.4.

〔57〕 控制概念倾向将隐私联系于个人的偏好和欲望,在这种理解下,隐私概念就可能根据个体喜好而变化,这导致隐私概念变得不稳定与易变,个体也可能对隐私提出各种不合理的要求,因此可能成为一个“反社会”概念。Solove, supra note 40, p.70. 对隐私权的负面评价,see Richard Posner, “The Right of Privacy”, *Georgia Law Review*, Vol.12, No.3, 1977, pp.393－422.

〔58〕 Nissenbaum, supra note 27, p.98.

〔59〕 美国隐私法的第三方原则即源于这一观念:一旦选择分享数据,就不能再去抱怨它被第三方分享。Hildebrandt, supra note 18, p.189. 在这种观念下,仅仅使用互联网本身,就可能意味已主动将自己的数据让渡给不受限制的数据控制者以及不特定的第三方,其后果是使大量个人信息置于隐私保护范围之外。Waldman, supra note 5, p.64.

控制范式成为当代隐私法的核心原则，强调个人信息“应完全由其所有者控制”。〔60〕1970 年代以降，隐私法经历了由数据控制者主导转向数据主体自我控制的观念变迁，“告知—选择”成为落实信息自我控制权的主要法律工具。〔61〕在美国，联邦隐私政策就主要依循控制范式，联邦贸易委员会(FTC)将“告知”作为公平信息实践原则的核心要素，数据控制者起草与发布相关的隐私政策，进而由数据主体对相关数据活动做出同意，“‘告知—选择’被内建为数据控制者和数据主体的基础法律关系”。〔62〕与此相应，欧盟的个人数据保护路径，也坚持将数据主体的同意作为数据处理的基本前提，“数据主体有权自行决定应在什么范围内将个人数据告知他人”。〔63〕美国的隐私自主与欧盟的信息自决，最终在控制这一概念上形成了范式合流。

二、巨变：信息隐私权的规范危机

(一)信息技术与隐私规范的内在张力

隐私概念变迁反映信息技术的发展，新技术蕴含了隐私侵犯的新手段，因而催生了法律概念演化。〔64〕近代隐私是印刷术的产物，是在私人书房安静阅读从而发展出丰富内心生活这一实践带来的副产品。〔65〕19 世纪晚期的照相与大众媒体等信息侵入技术破坏了印刷时代的信息规范，因而发展出强调隔离和独处的隐私概念，以保护私人生活免受外部侵扰。控制范式的理论源头，则可以追溯到上世纪七十年代，著名隐私法学者阿兰·威斯汀提出，隐私乃是不同主体对于信息沟通过程的一种自我控制权。〔66〕它所应对的，其实是二战之后出现的电子数据库技术，数据保密、数据最小化、告知—同意、退出权等原则，针对的都是数据库和计算机管理自动化带来的威胁，沃伦和布兰代斯时代的“独处”概念已无法应对这些新挑战。〔67〕电子数据库的技术特点，使其可以通过赋予个人信息控制权实现隐私保护：因为电子数据库是机械应用预先设定的计算规则，具有逻辑上的确定性。在这种技术模式下，隐私主要是各类可识

〔60〕 Luciano Floridi, *Information Ethics*, Oxford: Oxford University Press, 2013, p.241.

〔61〕 “告知—选择”原则出自 1973 年由美国联邦住房、教育和福利部起草的报告所发展的“公平信息实践原则”(FIPPs)。随后，联邦贸易委员会推动国会要求商业网站将“告知”作为最重要的公平信息实践原则。“告知—选择”最终通过一系列联邦和州的部门式数据隐私立法得以落实。Waldman, supra note 5, pp.30, 79, 80.

〔62〕 Waldman, supra note 5, p.31.

〔63〕 Tamò-Larrieux and Seyfried, *Designing for Privacy and Its Legal Framework*, Cham: Springer, 2018, p.81.

〔64〕 Durante, supra note 32, p.122.

〔65〕 Stalder, supra note 3, pp.1—15.

〔66〕 “隐私是由个人、团体或机构自行决定何时、如何以及在多大程度上将有关自身的信息传达给他人的一种权利。”See Alan Westin, *Privacy and Freedom*, New York: Atheneum, 1967, p.7.

〔67〕 同样，普罗瑟仅仅关注侵权法，而且他的著作完成于 1960 年，时值信息时代来临之前。因此，今天的许多隐私问题都不能被普罗瑟的四个类型涵括。Solove, supra note 40, p.101. 而在当前，传统隐私问题逐渐被信息隐私和个人数据保护问题取代，隐私范式则从隔离转向控制。

别的机器可读数据，信息处理过程是高度结构化的，可以被稳定预期从而实现个人控制。〔68〕申言之，在进入 1970 年代之后，隐私保护无法再简单依靠空间上的封闭与隔离，相反，主体必须参与和控制信息的流动过程。

这便是沿用至今且影响深巨的公平信息实践原则与个人数据保护框架的基本技术假设和规范预设，它解决的是电子数据库时代的信息隐私保护问题。在这种技术条件下，可以有效区分数据主体（数据处于危险中）、数据控制者（控制处理目的）和数据处理者（在数据控制者监督下操作数据）；规定处理条件（例如目的特定化、数据完整性）；对数据控制者施加信息义务（例如透明性、可审核性）；赋予数据主体权利（如访问、修改或删除个人数据的权利），总之，“控制范式充分体现于目的限制性、同意和数据最小化这些核心原则”。〔69〕

有史以来，从口传文化到书写时代，从印刷术、照相术再到电子数据库，信息技术变革一再凸显隐私边界的不确定，以及隐私保护的脆弱性。而晚近的大数据、云计算、物联网、人脸识别等技术发展更是从根本上挑战了建立于 1970 年代的信息隐私框架，“数据最小化、数据控制权与程序化问责等原则都不再适用”。〔70〕网络爬虫、个性广告、移动通信监控、应用程序捕捉实时位置、网络社交数字画像；数据处理系统的隐匿、数据收集规模的暴增、数据交换和转移速度的加快以及无限制的数据存储能力；〔71〕无线射频感应器与生物识别设备相互增强，与在线数据库软件连接，进行不间断实时分析，“在线世界以看似无限的能力收集、聚合、存储和挖掘行为数据，从而整合线下世界，创造出虚拟与物理现实的新融合”。〔72〕概言之，与电子数据库技术不同，新信息技术发展表现出以下特征：首先，它不再依赖“独立设备”，而是通过持续的互联，“这种互联允许捕获和存储大量琐碎的数据，然后挖掘出相关的模式”。〔73〕其次，机器不再仅仅感知环境（读取文本），还折返于环境（预测并应用结果）、建立反馈（比较预测和实际结果）、重新配置算法程序并改进表现。〔74〕其三，无论是移动、温度、面部表情、声音、语音、步态，包括同一环境下的过往，以及其他环境下的历史行为，全都成为新技术收集和分析的对象。〔75〕其四，数据挖掘不再仅仅表征当前事态，它还从过去的行动进行推断，从而预测未来的行为。〔76〕

更棘手的是，新信息技术不仅给我们带来巨大的隐私风险，而且还导致我们“缺乏信息工

〔68〕 See Mireille Hildebrandt, “Law as Information in the Era of Data-Driven Agency”, *The Modern Law Review*, Vol.79, No.1, 2016, p.9.

〔69〕 Mireille Hildebrandt, “Balance or Trade-Off? Online Security Technologies and Fundamental Rights”, *Philosophy & Technology*, Vol.26, No.4, 2013, p.368.

〔70〕 Hildebrandt et al., supra note 7, pp.196－197.

〔71〕 Larrieux et al., supra note 63, p.6.

〔72〕 Gutwirth et al., supra note 34, p.23.

〔73〕 Mireille Hildebrandt, “Legal Protection by Design: Objections and Refutations”, *Legisprudence*, Vol.5, No.2, 2011, p.227.

〔74〕 Hildebrandt, supra note 68, pp.9－10.

〔75〕 Hildebrandt, supra note 73, p.227.

〔76〕 See Gutwirth et al. (eds.), *European Data Protection: Coming of Age*, Dordrecht: Springer, 2012, p.289.

具去意识到这些问题，也缺乏法律与权利工具去寻求救济”。〔77〕概言之，1970 年代以来建立的信息隐私保护框架，主要立足于当时的信息技术条件，主要关注个人数据以及可能的滥用和控制。新信息技术正在迅速瓦解控制范式的技术假设，进而对信息隐私权的规范基础形成全面冲击与挑战。兹以大数据技术为例。

(二)大数据技术与隐私规范基础的瓦解

第一，大数据技术与信息隐私权的个人本位形成冲突。首先，人不再是原子化的，与世界隔离的形象，人成为高度社会化的实体，成为网络世界的节点。数字画像不再是“关注特定个体的数据，而是大规模人群的集成数据”。〔78〕其二，大数据技术主要通过不特定目标抓取、收集和处理不确定数量群体的信息，不再直接针对个体，而是在集合、群组与类型意义上统计其相关性。〔79〕第三，个人成为各种类型化标签的数据点，算法决策不需要与有血有肉的个人发生联系，而主要基于非个人、离散和可再分的各种数字轨迹，进而“形成超主体与亚主体的‘统计学身体’”。〔80〕第四，真实个体不断被涵括到统计画像的算法之中，他们不清楚自己是何种群组的哪一部分，也缺乏与编入这些群组的其他成员的互动。〔81〕第五，隐私侵权逐渐发生于群体层面，潜在的隐私侵害可能并未涉及任何具体个人，但它深刻影响所有人的所处环境，从而侵犯不特定群体的利益。〔82〕

第二，大数据技术腐蚀了信息隐私权的传统范式基础。其一，洛克范式认为隐私是隔离、独处的权利，在这种理解下，信息公开即是对隐私的“处分”和“放弃”。而在大数据时代普遍连接、公开与分享的条件下，洛克范式就可能给隐私保护带来自主放弃的悖论后果。同时，新技术条件下，个人数据很难再是洛克意义上的“排他性权利”，数据通常被大量人群共享，“数据主体”往往也无意进行“独占”。特定场景下，不同主体往往可以同时对同一数据主张不同权利。〔83〕其次，大数据技术已深度介入并支配数字人格与身份的设定，“在大数据画像中，人们将难以理解和回应自身如何被定位、涵括、排除、奖赏或是惩罚”。〔84〕康德范式的自主理论遭遇危机。

第三，大数据技术冲击了信息隐私权空间、事物与主体的维度假设。首先，传统隐私的空间边界是固定和可见的，而当前的信息沟通主要发生在“在线世界”与“大数据空间”，这是由数据服务器、推理机器和虚拟机连接的庞大网络，形成由各种分布式节点构成的复杂动态空间。〔85〕以往的隐私侵犯多发生于固定的空间，而在新技术条件下，信息流动变成非线性的动

〔77〕 Taylor et al., supra note 12, p.233.

〔78〕 See Mireille Hildebrandt and Bert-Jaap Koops, “The Challenges of Ambient Law and Legal Protection in the Profiling Era”, *The Modern Law Review*, Vol.73, No.3, 2010, p.434.

〔79〕 Sloot, supra note 9, pp.2—3.

〔80〕 Hildebrandt et al., supra note 7, p.157.

〔81〕 Taylor et al., supra note 12, p.145.

〔82〕 Sloot, supra note 9, pp.6,92.

〔83〕 See Luciano Floridi(ed.), *Protection of Information and the Right to Privacy——A New Equilibrium ?*, Switzerland: Springer, 2014, p.37.

〔84〕 Hildebrandt, supra note 18, p.91.

〔85〕 Floridi, supra note 83, pp.35,43.

态过程，难以事先在空间层面对信息的特征、功能与使用方式做出规定与评估。其次，在事物维度，传统隐私是一种确定的存在，具有客观、稳定和可预期的指向，而当下的信息流动则呈现暂时性、瞬时性，伴随时间持续变化的特征。“数据可以被回收、整理、匹配、重组……任何对信息的认知操作都是施为性的：它通过自动复制信息来改变信息的性质。”〔86〕同时，信息的循环生命周期也发生了深刻改变：信息起初是作为脱敏数据，但在与其他数据的连接中，则可能再次转变为敏感数据，而在群体画像中，它有可能被进一步集合并匿名化，而个人也可能再次被链接回这一画像过程。其三，在主体维度，数据生产者、收集者、处理者与消费者之间形成复杂的信息关系。隐私主体不清楚自己何种数据被存储，也不知道如何要求数据控制者开放权限；“隐私侵犯主体也可能消失，没有一方能为预测性算法结果承担相应责任”。〔87〕

第四，大数据技术侵蚀了信息隐私权的传统二分法。其一，私人/公共空间二分法被打破，“由于不断变化的态度、机制、现实条件和技术，公共与私人的界限不断发生演化”。〔88〕私人和公共的空间划分在网络世界不断模糊化，一系列公私领域的边界被无缝穿越。在离线世界之外，不断生成的网络空间(cyberspace)以及信息化的模拟空间，共同构成一个跨越公私领域的“信息圈”(infosphere)。〔89〕其次，私人/公共信息二分法模糊化。在新技术条件下，信息的类型和属性可能发生迅速改变，无论是私人数据、敏感数据、集合数据或公共数据，其信息类型都不再固定不变。〔90〕匿名数据可以回归为个人数据，公共信息也可能还原为个人信息。概言之，由于无法预知哪些数据会与其他数据关联，以及在数据处理过程中会产生何种新的知识，这些都导致私人/公共信息二分法失效。第三，私人/公共主体二分法被打破。在大数据技术背景下，私人利益开始难以“个体化”定位，与此同时，公共利益也难以被“特定化”。〔91〕在一些数据挖掘活动中，即使个人没有被“识别”出来，他们仍然可以被“触及”，并因此受到相应算法推断的深刻影响。〔92〕不同社会组织在大数据处理中承担的角色愈益模糊，信息流动过程变得高度复杂化，不同“权力”主体参与其中，侵权归责因此变得越加困难。关键是，无处不在的计算装置不再只是“公权”范畴，大量私人组织、资本和企业参与其中，从而形成复杂的公—私、私—私权力网络。概言之，私人/公共二分法隐含的一系列假设被新的技术发展削弱，从而难以继续作为隐私保护的规范基础。

第五，大数据技术挑战了信息隐私权的传统解释理论。其一，大数据主要从标签类型(乘客、年轻消费者、中产白领、低收入妇女等)而不是人格符号(你、我、他)来定位主体。〔93〕人格

〔86〕 Floridi, supra note 60, pp.259－260.

〔87〕 Hildebrandt et al., supra note 7, p.100.

〔88〕 Solove, supra note 40, p.50.

〔89〕 Durante, supra note 32, p.8.

〔90〕 See Ronald Leenes et al.(eds.), *Data Protection and Privacy: (In) visibilities and Infrastructures*, New York: Springer, 2017, p.5.

〔91〕 Sloot, supra note 9, pp.3－4.

〔92〕 Taylor et al., supra note 12, p.20.

〔93〕 Taylor et al., supra note 12, p.97.

理论与大数据技术模式发生错位。〔94〕其二，传统隐私权可以归属到特定个体，但在新技术环境下，一个个体在特定时间可能是数百个临时群组的成员，在法律上赋予所有这些群组身份以相应权利来保护隐私，在实践上不具操作性。由此，隐私的权利理论也遭遇困境。其三，若将隐私视为所有权或利益，也忽视了隐私保护深深依赖于特定的社会结构、技术基础设施和法律框架。隐私作为“财产”与“利益”不是自明的，它是特定技术背景下法律建构的产物，大数据时代的隐私危机深刻凸显了这一事实。

第六，大数据技术瓦解了信息隐私权的核心概念。其一，传统隐私的“独处”概念预设个人是原子化的，可以与他人和周围环境保持“隔离”。而新技术背景下的隐私则不具备这一可能。其二，隐私保护也无法再局限于“秘密”，因为数据处理过程具有动态性和循环性，加密数据可以轻易“去匿名化”与“再识别化”，公开数据也可能被挖掘出私密信息。其三，作为“接近”（访问）的隐私概念也变得不适用，因为大量信息收集、存储和处理活动并不需要实质的“接近”。〔95〕由于数字算法可能受知识产权或商业秘密保护，数据主体则往往无法“访问”这些算法程序。其四，隐私的人格概念受到挑战，因为人格开始“由智能冰箱的持续预期、输入信息的智能过滤、自适应交通管理或先发制人的健康监测无意识地塑造”。〔96〕其五，隐私也难以完全掌控“亲密关系”，各类机器算法正深度介入社会关系的建构。其六，控制概念逐步失效，大量数据在个人掌控范围之外收集与储存，大量数字踪迹散布在控制之外，“人们越加不可能对每一信息片段施加控制”。〔97〕大数据技术制造了“自主性陷阱”：即使自以为做出一个有意识的选择，但它潜在受到画像者和被画像者之间知识不对称的影响。〔98〕即使是自主决策，但“选项已经被格式化，以适应他被推断出来的倾向”。〔99〕而其结果是，越坚持控制概念，就越可能“悖论地走向数据主体对隐私的自主‘放弃’”。〔100〕

（三）技术巨变重构社会图景

信息技术发展深刻挑战了隐私权的规范基础，破坏了法律保护隐私的能力。〔101〕大数据技术不断将社会信息转译为离散的机器数据，诸如人脸识别、基因信息、社交数据、移动轨迹，以及与这些匹配发展的分析方法，例如云计算、机器学习与算法挖掘，都构成了隐私的新威胁。

---

〔94〕“如果环境剥夺了我们预见别人如何期待我们的可能性，那么我们发展自己身份的自由就岌岌可危了”。See Mireille Hildebrandt, “Who Needs Stories if you Can Get the Data ?ISPs in the Era of Big Number Crunching”, *Philosophy and Technology*, Vol.24, No.4, 2011, p.371.

〔95〕Solove, supra note 40, p.21.

〔96〕Hildebrandt, supra note 73, p.232.

〔97〕Taylor et al., supra note 12, p.46.

〔98〕T. Zarsky, “‘Mine Your Own Business !’: Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion”, *Yale Journal of Law & Technology*, Vol.5, No.1, 2002, p.17.

〔99〕Hildebrandt, supra note 73, p.233.

〔100〕Waldman, supra note 5, p.32.

〔101〕物联网结构化的数据分享会瓦解告知—同意这样的数据保护机制。Leenes et al., supra note 90, p.64.

技术发展不仅重塑了社会关系，“也改变了法律所保护的权利的本质和属性”。〔102〕因此，为了应对新技术挑战，重构信息隐私权的规范基础，就需要重新理解社会变化，考察技术发展带来的巨变，以及由此引发的隐私问题的复杂性。笔者试从空间、时间与社会三个维度简要分析。

首先，我们今天所处的是一个普遍化的计算环境和智能空间，它具有如下特点：其一，敞视性。以往，空间消极记录我们活动的痕迹，它是被动的，并不构成隐私的威胁。但在今天，各种广泛使用的工具和设备，全天候、全覆盖记录我们的行踪，将记录提供给“第三方”，庞大而普遍的数据收集形成了一个新型的敞视社会。〔103〕其二，规模性。“社会计算”编程将大量人群与机器整合其中，“新技术嵌于庞大的物理、社会和意义网络”，〔104〕这使空间容纳的信息沟通规模与挖掘深度大为提高，个人与群体、社会和机器全都成为网络调动的节点，由此形成的不再是牛顿或康德的空间概念，而是去中心、混合性（物理和虚拟）、既扩张又收缩、计算性与信息化的空间意象。〔105〕其三，智能性。空间发展为由不同主体实时沟通和交换信息的智能场所。诸如人工智能、物联网、智慧城市相互连接，实时收集、处理与共享数据，“机器成为我们大多数沟通的中介”，〔106〕空间自身形成了“自我控制和自我规制的能力”。〔107〕其四，穿越性。离线世界与在线世界持续分化并深度耦合，在这一双重空间进行信息沟通的是不断激增的人—机关系所形成的复杂网络，各种不可见的计算决策系统，打破了现实空间和网络空间的传统界限。〔108〕其五，多变性。栖居新空间的主体包含各类计算实体与信息实体，其特征是高度的“流动性、可转移性和结合性”。〔109〕它们不再具有确定与有形的边界，而呈现模块化、组件化、插件化，具有“可分解性和去植根性”。〔110〕其六，黑箱性。新空间遍布各种复杂的算法机制与人工神经网络，海量的数据，包括个体行为模式、集群、眼球运动、天气状况、产品周期管理、皮肤状态、步态、人脸、金融交易、安全漏洞、血液构成，都通过各类计算机器进行挖掘、收集、建构、读取和评估，而这些数字黑箱的技术原理却鲜为人知。第七，跨国性。信息社会的流动性特征创造了一个跨越国家的全球信息网络，隐私问题成为超国家和全球化现象。传统的国家法与国际法管辖效力出现失效，经济系统和科技系统的功能逻辑不断扩张，“主宰与支配其他

〔102〕 Durante, supra note 32, p.118.

〔103〕 See Bauman, Zygmunt and David Lyon, *Liquid Surveillance: A Conversation*, Cambridge: John Wiley & Sons, 2013.

〔104〕 Nissenbaum, supra note 27, p.6.

〔105〕 See Luciano Floridi, “Global Information Ethics: The Importance of Being Environmentally Earnest”, *International Journal of Technology and Human Interaction*, Vol.3, No.3, 2007, pp.1－11.

〔106〕 Ryan Calo, “People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship”, *Penn St. L.Rev.*, Vol.114, No.3, 2010, p.809.

〔107〕 Durante, supra note 32, p.127.

〔108〕 See Luciano Floridi, *The Fourth Revolution: On the Impact of Information and Communication Technologies on Our Lives*, Oxford: Oxford University Press, 2014, p.41.

〔109〕 J. Kallinikos, *The Consequences of Information: Institutional Implications of Technological Change*, Cheltenham: Edward Elgar, 2006, p.18.

〔110〕 Ibid., p.15.

领域乃至整个社会的逻辑”。[111]

其次，新信息技术的深刻影响也从空间维度不断延伸向时间维度，表现为以下特征：其一，实时性。电子数据库时代的重点是记录“过去”（档案、数据库等），而新技术环境不再只是关注过去的痕迹，也聚焦发生在当下的沟通。对于“当下”的知识，是“基于实时的数据收集，而不是基于对过去痕迹的重构”，[112]由此形成了一个适应持续变化环境的实时系统。其二，跳跃性。数据交换过程同步化，包含大规模的平行处理。信息不仅从一个领域转移到另一个领域，还经常跨越时间线，过去收集的信息（甚至是久远的过去）被重新注入到当下情境。[113] 其三，动态性。个人身份“不再是在一个单一时间框架内一劳永逸地建构，而是动态、连续的过程”。[114]人格“继发性的多阶段发展过程被即时性的干预和调整所取代”。[115] 其四，前瞻性。大数据不断形成对未来的推断，基于未来推断建立数字模型，进行假设、预测与引导，并以此检视和评估当下。“对于‘当下’的知识与评估，受制于对‘未来’的推断和预期”，时间焦点从过去和当下转向未来。[116] 其五，丛集性。新信息技术同时介入对过去、当下和未来时间维度的操作，三种维度并不相互排斥，而是丛集并存。由此形成的历史隐私、实时隐私与推断隐私，给隐私保护带来前所未有的挑战。其六，时间性。大数据空间本身就是时间化的空间，空间隐喻趋于消失，“隐私越来越少出现在拓扑术语中（这里/那里），而更多出现于时间术语中（之前/之后）”。[117]

复次，新信息技术也深刻重塑了社会维度：其一，社会主体。各种不可见的复杂数据模型，不断切割和再组合个体，数字主体而非血肉之躯成为重点。[118] 数字主体形成沟通潜力，而行为结果“越来越难以被归因到一个独立、中心化和自主性的行动渊源”。[119] 其二，社会行动。数据挖掘和模型技术相互结合，根据不同场景，预测与干预人们的行为和运动。通过改变参数，这些模型可以“持续改变行动的反馈闭环”，进而改变个体的行为决策。[120] 其三，社会交互。新信息技术催生了一系列多主体系统（multi-agent systems），主体不再必然是人类，也可以是组织、人工主体或混合系统。收集和处理信息活动不再仅由单个（人或人工）主体，也开始由超主体、多主体系统或分布式与普遍系统（自动计算

〔111〕 Floridi, supra note 83, p.44.

〔112〕 Durante, supra note 32, p.127.

〔113〕 See Helen Nissenbaum, “Protecting Privacy in an Information Age: The Problem of Privacy in Public”, *Law and philosophy*, Vol.17, 1998, p.585.

〔114〕 Durante, supra note 32, p.138.

〔115〕 Serge Gutwirth, *Privacy and the Information Age*, Lanham: Rowman & Littlefield, 2002, p.76.

〔116〕 Durante, supra note 32, p.127.

〔117〕 Durante, supra note 32, p.128.

〔118〕 Solove, supra note 40, pp.119, 125.

〔119〕 Durante, supra note 32, pp.45－46.

〔120〕 Hildebrandt et al., supra note 7, p.58.

系统)完成。[121] 其四,社会权力。过去,国家是信息生命周期的主要管理者,隐私保护主要针对公权力。新技术条件下,国家不再是处理、控制和管理信息生命周期的唯一实体,信息寡头企业获得过滤、聚合与协调信息的强大权力,成为隐私侵犯的重要威胁。其五,社会归责。传统隐私聚焦于特定的侵害,进行个体化的法律归责。但新技术变革使隐私侵犯变为由大量细碎操作或黑箱程序带来的系统性权力问题,"责任弥散在大量行动者之间,它们具有完全不同的动机与目标,每一方在不同时间点都发挥着不同的作用"。[122] 在这种背景下,明确的隐私侵权者变得难以定位。

三、再造隐私:信息隐私权规范基础的重构

(一)信息论与社会理论视角下的隐私

在信息论视野下,隐私并不是一组客观的数据,而是一种信息化的能力,它具有封装和支配数据的能力,可以不断把数据转化为信息,并赋予其意义。正是在这个角度,本文强调信息隐私权而不是数据隐私权,以突出隐私权的信息性、社会性、关系性和能动性特征。从社会理论视角分析,隐私是法律对信息稀缺性的人为建构,以此确立隐私信息的独特价值,将其区分于一般的数据信息。因为,隐私是现代社会确立个体人格的重要工具。换言之,保护隐私,也是保护与创造法律人格的稀缺性,从而为现代社会运行提供宝贵的自由主体(agent)资源,这是现代人类作为个体存在的信息论前提。信息作为"制造差异的差异",[123]其本质即在于区分(distinction),而隐私则构成主体建构自我身份的基础,以此成就法律人格的独特性。表面上,隐私保护与信息流动存在矛盾,但实际上,没有稀缺性就没有冗余性,信息社会信息的冗余性和弥散性,恰恰悖论地建立在隐私信息的稀缺性与差异性之上。

进言之,隐私并不是固定的事物,而是一束可变的信息关系。信息隐私比个人数据拥有更为丰富和复杂的内涵,它"保护我们将数据转化为与自身相关的信息的能力",[124]也因如此,隐私"不只是一种利益或偏好,也具有价值与道德含义"。[125]

社会演化不断产生新的信息规范。信息社会创造了新的信息类型、行动者类型以及沟通模式,这也要求我们在理论上为信息隐私权提出新的规范框架。在传统时代,隐私

---

[121] See Ugo Pagallo, "Robotrust and Legal Responsibility", *Knowledge, Technology & Policy*, Vol.23, No.3, 2010, pp.367－379; Giovanni Sartor, "Cognitive Automata and the Law: Electronic Contracting and the Intentionality of Software Agent", *Artificial Intelligence and Law*, Vol.17, No.4, 2009, pp.253－290.

[122] Solove, supra note 10, p.61.

[123] G. Bateson, *Steps to an Ecology of Mind*, St Albans: Frogmore, Paladin, 1973, p.319.

[124] Durante, supra note 32, p.132.

[125] Nissenbaum, supra note 27, p.66. 波斯特也坚持隐私的规范面向,认为规范性含义内在于其概念核心,否认隐私作为描述性中立概念存在的必要性。See Robert Post, "The Social Foundations of Privacy: Community and Self in the Common Law Tort", *California Law Review*, Vol.77, No.5, 1989, pp.957－1010.

被固定于静态化的空间和人格，而在信息时代，空间与人格是多重、可塑和易变的，“我们每个人都成为信息系统，在一个由信息构成的环境中，与其他信息系统进行信息的生产、处理和交换”。〔126〕人们在信息沟通与数据流动中不断形成新的认同，隐私不再是固定不变的实在，而是嵌入到高度流变的网络关系中。因此，我们需要从信息论和社会理论视角重新理解隐私，进而对信息隐私权的规范基础进行重构：从个人本位转向社会本位；从控制范式转向信任范式；从独占维度转向沟通维度；从二元对峙转向一体多元；从权利视角转向权力视角；从概念独断转向语用商谈。

（二）信息隐私权规范基础的重构

第一，从个人本位转向社会本位。传统上认为隐私和社会是对立的，“隐私意味个人的优先性以及个体权利对于社会的超越性”〔127〕“隐私权本质上是一种躲避集体生活的权利”。〔128〕但在社会理论视角下，隐私绝不是与社会隔离的概念，许多学者都强调了隐私的社会本位与关系主义视角。齐美尔指出，隐私是一种“普遍的社会形式”，是一种用来帮助界定社会关系的社会形式。〔129〕戈夫曼同样强调隐私的社会角色和社会价值。〔130〕罗伯特·波斯特则认为，隐私侵权并非社会对个人的伤害，而是对人际相互依赖性与社会形式的一种破坏。〔131〕换言之，社会理论视角的隐私理论洞察到隐私所承担的重要社会功能，认为隐私构成了社会结构的基础要素。正如当代心灵哲学所揭示，自我乃是一种涌现现象，它并不起始于个体，而是在复杂的社会过程中同时茁生了自我与他者。〔132〕信息不是由个体独立创造，信息产生于社会主体的互动。因此，个人绝不是原子化的个体，而是“作为在不同社会语境中处于具体社会关系，参与具体社会活动的具体社会成员”。〔133〕实际上，有学者研究揭示，隐私权最初并不定位于个体权利，而主要聚焦社会的一般利益和公共利益。在法律实践中，经历了从数据控制者的一般义务到数据主体的主观权利，从一般社会利益到个体利益视角的转变，隐私保护的个人本位并不是先天的。〔134〕学者里根更是认为，隐私乃是“公共品”，与清洁空气和国防一样，隐私最好通过公共监管来保护，而不只是借助私人机制。〔135〕其关键是，在新技术背景下，隐私侵权的发生机理已与法律救济的个体机制发生严重错位。为了应对技术变革带来的系统问题，隐私的

〔126〕 Durante, supra note 32, forward, vi.

〔127〕 Waldman, supra note 5, p.11.

〔128〕 Solove, supra note 40, p.89.

〔129〕 Georg Simmel, “The Secret and the Secret Society”, In Kurt H. Wolff(ed), *The Sociology of Georg Simmel*, translated by Kurt H. Wolff, New York: Free Press, 1950, p.338.

〔130〕 See Erving Goffman, “The Nature of Deference and Demeanor”, *American Anthropologist*, Vol. 58, No.3, 1956, pp.473－502.

〔131〕 在这种新的理论视角下，隐私原告就不是个人受害者，而是社会规范受害群体的代表者。Post, supra note 125, pp.957－1010.

〔132〕 Richardson, supra note 14, p.19.

〔133〕 Nissenbaum, supra note 27, pp.129－130.

〔134〕 Sloot, supra note 9, p.1.

〔135〕 See Priscilla M. Regan, *Legislating Privacy*, Chapel Hill: University of North Carolina Press, 1995, p.221.

价值本体有必要重归社会视角，致力从一般利益、社会利益和公共利益定位隐私，化解个人与社会的二元论，不仅“考虑个体的具体伤害，也应当考察社会层面的潜在伤害，不仅应该考虑相应的法律后果，也要重视相应的伦理和社会后果”。〔136〕

第二，从控制范式转向信任范式。隐私权的洛克与康德范式，都强调主体对个人信息（数据）的占有、控制和处分，在当代浓缩为控制范式。而在当下，我们已经很难将任何信息进行独占，对于信息流动更是无法实现“控制”。因此，重要的不是与社会的隔离，而是如何基于信任进入社会。在信息流动和分享的语境下，信任意味着在披露个人信息过程中，自愿在他人面前呈现脆弱性。因此，每一种信息关系实际都包含着一定程度的信任，只有当人们相信对方是值得信任的，才更有可能去分享信息。所以，隐私“是在社会分享者之间建立信任的一种社会建制”。〔137〕隐私虽然对个人信息流动构成限制，但它绝不是单向的控制，它的目标是在复杂的社会网络中，给社会生活的不同领域带来平衡。“如果说个人数据是当代全球经济的货币，那么信任就是中央银行。”〔138〕我们需要发展隐私理论，建立与相互信任的信息关系及促进信息分享的技术发展趋势相适应的理论范式。而在建构信任范式中，最重要的是确立信息受托者的可信任性。学者巴尔金提出了“信息信托”这一重要概念，因为，所有信托法都基于两项前提：不对称性和脆弱性。只有在受托人尽职照顾信托人利益的情况下，才能赋予受托人相应的权力。“如果你让另一个人对你产生信任，你不能转身背叛这种信任。”〔139〕在新技术条件下，由于信息权力不对称如此显著，就迫切需要引入类似信托这样的法律概念，来重新构建信息隐私的信任关系，推动个体与个体、个体与互联网公司、个体与社会修复信任关系。

第三，从独占维度转向沟通维度。传统隐私权聚焦空间、事物和主体维度，形成隐私独占的意象。而在信息论视角下，有必要强调隐私的事物、社会与时间维度，建立能够促进信息沟通、互动和共享的规范框架。沟通维度呼应于当代信息社会的发展趋势，将关注焦点从隐私隔离转向信息流动。易言之，沟通维度观察到各类原始数据、网络数据和处理数据在机器、人机、人—人之间的快速流动，关注到信息对于信息主体、受体、发送者、接收者与指涉者的不同含义，将隐私纳入关系化和网络化的视角，从控制论、博弈论、信息论视角审视交互计算背景下隐私关系的互动性与时间性特征，进而审思由此形成的权力结构和法律责任。〔140〕不同社会演化出不同的信息环境，由此也产生了不同的行动者与归因配置，并因此形成信息规范的不同特征变量。在信息论视角下，信息规范至少由三大变量构成：行动者、信息类型与传输原则。行动者具有不同社会角色，信息类型则根据语境和场景变化，传输原则也包含众多。〔141〕因此，隐私权绝不只是单一的主体、秘密或控制视角，而是信息“恰当”流动的权利，在其背后，蕴含着

〔136〕 Sloot, supra note 9, p.102.

〔137〕 Waldman, supra note 5, p.149.

〔138〕 Gutwirth et al., supra note 76, p.177.

〔139〕 Jack Balkin, “Information Fiduciaries and the First Amendment”, *UC Davis Law Review*, Vol.49, No.4, 2015, p.1224.

〔140〕 Durante, supra note 32, pp.56－58.

〔141〕 独占只是其中一种，还包括“秘密地”“第三方授权”“法律所要求的”“售出”“买入”“互惠”“经由证明的”等等。See Helen Nissenbaum, “Respecting Context to Protect Privacy: Why Meaning Matters”, *Science and Engineering Ethics*, Vol.24, No.3, 2018, p.840.

信息沟通的复杂规范体系。隐私是对“信息沟通和流动的一种赋权与限制”，〔142〕进言之，隐私“并非简单地限制信息流动，而是保证信息流动的适当性”。〔143〕因此，沟通维度可以让我们回到社会交往的具体场景和情境，聚焦特定的信息关系，以及与此种关系相适应的隐私期待、法律机制与保护方法，由此“构建一种几何多变的隐私保护体系，根据数据主体、数据处理者、数据类型、使用类型及其语境采取不同的保护方式”。〔144〕换言之，隐私的事物、社会和时间维度无法相互化约，没有任何一个维度可以单独垄断隐私的定义，正因如此，秘密范式、独占意象或控制概念都是片面的。

第四，从二元对峙转向一体多元。传统信息隐私权建立于私人/公共二分的古典自由主义理论，由于受到二分法理论束缚，隐私经常会被神圣化或污名化。〔145〕而在信息时代，私人与公共的二元界限正被不断打破，隐私无法再是私人领域对公共领域的孤立和隐藏，而必然是信息主体在不同时空语境下确立自我边界的连续动态过程。隐私本身就具有鲜明的公共属性与公共价值，确定隐私边界的过程就发生于社会领域，只有在群体关系中，才能确定隐私的真实含义。因此，将隐私片面等同于私人利益，将隐私对立于国家权威和公共利益，在实践中只会带来负面的后果。在当代，如果不能超越古典自由主义提出新的理论规范，就难以在新的技术背景下捍卫人的尊严。一方面，个体缺乏足够的知识和资源，另一方面，隐私问题高度结构化，不仅影响特定个体，也影响整个社会。“正因为问题是架构性的，所以解决办法也应当是架构性的。”〔146〕因此，只有构建一体多元的隐私命运共同体，才有可能创造可持续发展的信息社会。私人/公共二分法一方面忽视了隐私命运的一体性，另一方面也忽略了信息社会的生态多样性，将社会简单化约为两个二元对立的领域。作为“一体”，公民需要在隐私风险评估过程中获得充分参与权，采取多方利益攸关者路径，公共机构有责任在信息保护方面承担积极角色；作为“多元”，要求我们必须采取信息社会的生态主义视角，理解当代社会的功能分化趋势，改变经济部门和商业语境对隐私世界的殖民化。其关键是，将隐私的二元对峙转化为信息主义的统一视角，从信息生产、处理、沟通和分享的系统运作逻辑出发，充分考虑信息场景与语境的特性，周密评估信息属性、主体角色、信息关系、分享形式等特征变量，构建一个隐私友好的信息规范框架。〔147〕

第五，从权利视角转向权力视角。传统隐私权的化约主义、所有权、人格、功利主义和权利理论，都毫无例外地聚焦于信息弱势者视角(patient)，强调数据主体作为信息弱势者的主观权利(利益)；在新技术条件下，亟待将隐私保护转向信息强势者(agent)视角，强化数据控制者作

〔142〕 Waldman, supra note 5, p.34.

〔143〕 Nissenbaum, supra note 27, p.2.

〔144〕 Taylor et al., supra note 12, p.51.

〔145〕 比如，在波斯纳看来，隐私法导致人们隐藏有关自身的信息，从而“误导那些与之发生互动的人”。隐私造成了无效率、交易成本和伤害，“隐私变成了一种欺诈”。See Posner, *The Economics of Justice*, Cambridge: Harvard University Press, 1983, pp.231－233. 而在女性主义学者麦金农看来，(家庭)隐私构成对妇女平等的伤害，它是一种“让男人避开国家，任意压制妇女”的权利。See MacKinnon, *Toward a Feminist Theory of the State*, Cambridge: Harvard University Press, 1989, pp.184－194.

〔146〕 Solove, supra note 10, p.100.

〔147〕 Waldman, supra note 5, p.44.

为权力施为者的责任，这一责任不需要直接对应弱势者的权利。因为，隐私权本是应对信息权力不对称的一种法律工具，而在实践中，信息权力正不断倾向信息强势者，数据主体相对数据控制者的向上透明性愈益凸显，数据控制者的向下透明性则停留于名义，权力不对称越发严重。[148] 互联网企业在这种权力结构下更加追求短期利益，从而形成“鼓励将数据货币化的短期性和短视性的法律体制”。[149] 隐私的自我管理变成闹剧，“告知过剩，而选择缺席”；[150]各类隐私立法在执行过程中存在大量例外和漏洞，“法律很多，但保护很少”。[151] 根本原因就在于，传统隐私保护过多关注信息弱势者的权利，而未能关注信息权力的结构性问题。事实上，在劳动法、消费者保护、环境保护等法律领域，都早已将社会权力的不对称纳入视野，进而构建新的法律问责机制。在信息隐私权问题上，也迫切需要从权利视角转向权力视角，从承受者视角转向施为者视角，从数据主体的知情—同意转向数据控制者的可问责性（accountability）。在私法框架中，义务与相关的权利对应，而在公法框架中，法律义务和责任却不需要直接对接个体权利。在新的信息权力结构下，隐私权的规范基础亟需超越权利主义和私法主义的视角。

第六，从概念独断转向语用商谈。传统隐私理论都尝试从概念核心去界定隐私本质，由此陷入某事物处于隐私范围之内或之外的无休止争论，这导致隐私概念“要么过于狭窄而不够包容，要么过于宽泛而沦为模糊”。[152] 但按照当代语言哲学的理解，隐私不应在形而上、终极性、内在真实的语义学意义上把握，因为隐私首先是一种语用学和现象学表征，“隐私不是由（of）信息构成，而是通过（by）信息构成”。[153] 技术发展的不断加速，社会系统与社会场景的不断分化，有关隐私的定义、范围、保护程度和救济方式，不再有固定和统一的标准，而是表现为一整束具有演化特征的伞状型术语。无论是独处、接近、秘密、亲密、人格或控制概念，都不足以完整涵括隐私的本质。这要求我们从概念独断论走向语用性商谈，让信息主体不断参与到与自身息息相关的信息规范和隐私期待的公共商谈。“权利是关系，而不是事物。”[154]事实上，“隐私的合理期待”本身就是一个社会学概念，但在实践中，隐私的合理期待往往蜕化为“法院认为合理的期待”，从而无法真实反映社会的理解。[155] 隐私政策制定过程往往由官方与巨头企业垄断，广大消费者缺乏知情权和参与权。因此，我们应该转换思路，告别概念独断论，采取商谈进路重新定位信息隐私权。过时的语义学范式忽视了公共参与的巨大潜力。最关键的是，要为信息主体参与平等商谈提供各种渠道和途径，在持续的社会参与、公共舆论与权力监督的压力下，由相互理解的交往行动形成社会反制力量，进而发展出基于公共商谈的隐私规范体系。

---

〔148〕 Hildebrandt et al., supra note 7, pp.202－203.

〔149〕 Richards et al., supra note 23, p.435.

〔150〕 Richards et al., supra note 23, p.445.

〔151〕 Solove, supra note 10, p.71.

〔152〕 Solove, supra note 40, p.44.

〔153〕 Durante, supra note 32, p.86.

〔154〕 （德）哈贝马斯：《在事实与规范之间：关于法律和民主法治国的商谈理论》，童世骏译，三联书店 2003 年版，第 520 页。

〔155〕 Solove, supra note 40, p.72.

四、结语:信息隐私权的中国宪法时刻

保卫社会、缔结信任、促进沟通、一体多元、问责权力、公共商谈,信息隐私权的规范重构,还需要完成体系框架的根本定位。技术发展日新月异,信息规范不断演化,隐私保护同样需要升级更新,以促进信息社会的可持续发展。〔156〕 这要求超越单一的私法或公法视角,从宪制演化和基本权利的高度重新理解信息隐私权。

法国法学家瓦萨克(Karel Vasak)最早提出代际人权(the generations of human rights)的观念。所谓代际人权,是强调权利具有演化(evolutionary)、动态的(dynamic)的特质,其累积性(cumulative)和继发性(successive)特征是对社会变迁的回应。〔157〕 事实上,代际权利演化的观念,可以帮助我们解决隐私权与个人信息保护、数据权等性质和关系的长期争论。信息隐私伴随时间而演化,部分权利形态在此过程中消失,部分权利形式得以新生,这构成信息隐私的代际权利形态。这些权利形式不是互相取代与排斥,而是累积、重叠、依赖和交叉的关系。正是在历史演化中,信息隐私得以更新与发展,而不同形式的保护需求逐渐落实为多元的权利形态。因此,我们不妨将信息隐私权视为一个容纳不同代际隐私权的综合概念,作为权利演化树(evolutionary tree),信息隐私伴随技术发展不断衍生新的家族权利,建立起包括私法和公法在内的多部门复杂规范网络,从而成为一个统合性与涵括性的"大隐私"概念。

不同代际隐私具有相对独立的背景、传统和原理。易言之,隐私权演化回应了从个人社会到组织社会再到网络社会的结构化变迁。〔158〕 第一代隐私是个人消极自由的概念,预设侵权方与被侵权方的防范关系和平等主体关系(空间隐私/侵权隐私)。第二代隐私则是组织社会的产物,主要针对个人与各类公共、专业或商业组织之间持续的不对称信息关系(有关同意/自决、进入/退出的公平信息实践原则)。而当进入网络社会,技术平台取代各类人际互动和社会组织成为信息沟通的枢纽,信息权力超越传统的个人与组织视角,形成总体性的社会涵括和排除的权力效果,因此,也就特别需要发展出相应的隐私权概念予以制衡。如果说,第一代隐私主要借助侵权法机制,通过私法工具(个人—个人),保护"私人信息"(亲密信息/秘密信息/敏感信息);第二代隐私主要依靠公私法合作(个人—组织),保护"个人信息"(个人数据/数据主体);那么网络社会的第三代隐私,则需要演化为宪法性的概念(信息权力—权利的构成与限

〔156〕 我国在信息隐私保护领域存在立法碎片化、缺乏可操作规则等诸多问题。特别是,对个人信息和隐私两者关系的认识仍然存在分歧,时而陷入"一元制"和"二元制"保护模式的争论,在立法路径选择上摇摆不定。参见徐明:"大数据时代的隐私危机及其侵权法应对",《中国法学》2017 年第 1 期,第 130—149 页;李永明:"论《民法总则》中个人隐私与信息的'二元制'保护及请求权基础",《浙江工商大学学报》2017 年第 3 期,第 10—21 页。

〔157〕 See Karel Vasak, *The International Dimension of Human Rights*, Westport: Greenwood Press, 1982, pp.715—716.

〔158〕 有关个人社会、组织社会与网络社会,这里采用了德国法学家 Karl-Heinz Ladeur 的理论概念。See Karl-Heinz Ladeur, " Constitutionalism and the State of the 'Society of Networks': The Design of a New 'Control Project' for a Fragmented Legal System", *Transnational Legal Theory*, Vol.2, No.4, 2011, pp.463—475.

制)。隐私不再只是聚焦个人权利的私法规则,也不再只是强调知情同意的信息政策,而必须基于新的社会、技术和制度条件,成为宪法性的基本权利概念。〔159〕最关键的是,通过构建信息隐私的"权利树"与"法律树"体系,形成足以制衡各类不对称信息权力的宪制安排。〔160〕

隐私的传统民法视角聚焦个体权利与个人利益,但新的技术现实已然深刻影响结构性和社会性的利益。质言之,将隐私权定位于个人私权本位的民法视角已捉襟见肘。事实上,在欧洲,隐私既是国家层面的宪法权利,也是大陆范围的基本权利。〔161〕而通过连接民法与宪法的一般人格权概念,隐私保护早已突破狭义的民法框架。〔162〕同样在美国,隐私虽然最早是作为普通法权利,但《权利法案》在隐私案件中的分量也已变得越来越重。〔163〕进言之,欧盟《通用数据保护条例》建构的实际也是一个具有宪法性质的"二元治理"结构:一方面赋予个人正当程序权利;一方面通过合作治理结构制约信息权力。〔164〕传统隐私通过私法赋权,形成去中心的个人信息治理和执行机制,国家不承担建立专门机构监督与执行隐私保护的职能。〔165〕而在今天,单一的民法路径已无法有效承担信息治理的功能,隐私的私人执行机制已逐渐转向宪法化的合作治理机制。〔166〕

隐私不只是原子化的个人权利,它也有关信息权力的配置与运行。数据保护不只是告知、选择和控制,更需要直面"数据工业复合体"(data industrial complex)的负外部性。〔167〕正如前文所述,隐私的功能不只在于保护个体,它对于社会本身也具有重要的建构作用。因此,有

---

〔159〕基本权利不仅对国家权力,也对私人(私权力)施加义务的宪法理论在不同法系都已得到蓬勃发展,主要包括"国家行为理论""基本权利的横向效力""基本权利结构化效果理论""基本权第三人效力与放射效力"理论等,目前我国宪法学主要受德国第三人间接效力理论影响。See G.W. Anderson, "Social Democracy and the Limits of Rights Constitutionalism", *The Canadian Journal of Law & Jurisprudence*, Vol.17, No.1, 2004, pp.31－59;张翔:"基本权利在私法上效力的展开——以当代中国为背景",《中外法学》2003 年第 5 期,第 544－559 页。

〔160〕有关"权利树"与"法律树"概念,这里受到了王锡锌教授的启发。参见王锡锌:《〈数据安全法〉应考虑的三组关系》,载微信公号"人大未来法治研究院",2020 年 8 月 6 日上传。

〔161〕See Viktor Mayer-Schonberge, "Beyond Privacy, Beyond Rights——Toward a 'Systems' Theory of Information Governance", *California Law Review*, Vol.98, 2010, p.1862.

〔162〕《欧洲人权公约》第 8 条已成为作为基本权利的隐私权发展的基础条款,该条最初是典型的第一代隐私权,但通过司法实践,它已演化为积极的人格权概念。法院通过概念诠释,大大拓展了隐私涵括的范围,保护了大量原来从属于公约其他条款的权利与自由。德国的一般人格权与信息自决权概念也发挥了相似的宪法保护功能。德国法最初没有专门的隐私权民法概念,隐私性权益通过一般人格权得到发展。See Bart van der Sloot, "Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of 'Big Data'?', *Utrecht Journal of International and European Law*, Vol.31, 2015, pp.26－28.

〔163〕Ibid., p.26

〔164〕See Margot E. Kaminski, "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability", *California Law Review*, Vol.92, 2019, pp.1529－1616.

〔165〕Mayer-Schonberge, supra note 161, p.1872

〔166〕Mayer-Schonberge, supra note 161, pp.1856,1875.

〔167〕See Woodrow Hartzog and Neil Richards, "Privacy's Constitutional Moment and the Limits of Data Protection", *Boston College Law Review*, Vol.61, No.5, 2020, pp.1695,1725.

必要将隐私保护上升到信息社会宪法的高度进行认知。信息即权力，掌握信息即意味施加权力的可能。〔168〕当前，各类网络平台企业正在取得准主权实力，这些信息权力正在深刻塑造隐私的表现形式与可能性边界。所以，当代隐私不仅要从权利保护机制，更应当从构建和制衡信息权力的维度来定位它的宪法功能。仅仅只有权利清单，却没有相应的权力配置与制衡机制，就不足以成为宪法性的制度框架。如何塑造信息技术，如何规制信息权力，将对未来信息社会的宪制发展产生深远影响。

在信息社会，法律权力与权利的组织和配置都紧密围绕信息关系展开，因此，信息隐私权不再只是简单的私法或公法权利，而是具备了枢纽性的基本权利的意涵。〔169〕信息隐私的宪法化，最重要的不是简单将隐私权入宪，更关键的，是根据宪法机制的演化原理，为信息隐私保护寻找到根本的目标方向与价值定位。它既应当包含类似信息《权利法案》的实质性规则，又应当涵括针对信息权力、治理和责任的程序性规定。正如近代宪法对政治权力的构成性和限制性功能，信息隐私宪法化的核心任务乃是对信息权力在规范上的构成与限制，以促进信息社会的可持续发展。〔170〕

布鲁斯·阿克曼(Bruce Ackerman)认为，美国历史上存在着宪法身份根本再造的数次关键时刻。在日常政治的挤压和利益团体的压力下，立法者往往难以打破法律发展的常规；而在“宪法时刻”(constitutional moment)，人民被高度动员，广泛参与公共商谈，政治精英与人民大众深入互动，这让他们得以摆脱当下处境，去思考根本的秩序问题，从而深刻改变宪法发展的路径。〔171〕同样道理，我们当下正处于信息社会发展的关键时间窗口，当前的制度抉择将在未来几十年持续塑造法律演进的方向。中国信息隐私法发展面临重要的“宪法时刻”。

欧洲隐私法的快速发展就得益于它在宪法定位上的明确化。当前，我国信息隐私法的体系重构也迫切需要寻找宪法层面的根基，以信息权利保障与信息权力制衡为基本目标，为信息

〔168〕 See Austin Sarat (ed.), *A World without Privacy: What Law Can and Should Do?*, Cambridge: Cambridge University Press, 2014, p.65.

〔169〕 基本权利的具体功能包括：基本权(间接)第三人效力与放射效力、基本权作为组织与程序保障、基本权保护义务等，参见张嘉尹：“基本权理论、基本权功能与基本权客观面向”，载《当代公法新论(上)》，元照出版公司 2002 年版，第 50 页。

〔170〕 在德国法学家托依布纳看来，传统宪法的焦点在于释放政治权力的能量，同时又有效限制这种权力；而当前的宪法挑战，则在于如何释放各种超脱国家主权控制的不同社会能量(如经济、金融、科技和网络传媒)，同时又有效限制它们的破坏性。宪法问题已跨越国家层面，出现在各种“私人部门”中，宪法不再局限于纵向的“国家宪法”，也开始扩展为横向的“社会宪法”。为了更好保护个人，甚至保护各种社会体制，需要拓展制度化、组织化与系统化的保护渠道。借助社会理论，“宪法”可以进行更抽象的理解和表述。宪法化的判准包括宪法功能、宪法领域、宪法过程和宪法结构四个维度，通过这四个维度，宪法化实现对社会过程的正当化构造，确立起实质的宪法权威。参见(德)托依布纳：《宪法的碎片：全球社会宪治》，陆宇峰译，中央编译局 2016 年版；余成峰：“系统论宪法学的理论洞见与观察盲点——托依布纳《宪法的碎片：全球社会宪治》读后”，《政法论坛》2020 年第 2 期，第 134－142 页。

〔171〕 有关阿克曼的“宪法时刻”概念，可参见(美)布鲁斯·阿克曼：《我们人民：奠基》，汪庆华译，中国政法大学出版社 2013 年版。

隐私的民法、刑法和特别法保护建立一个统合于宪法的客观价值秩序框架。〔172〕目前我国法学界的通说认为,《宪法》第38条"人格尊严不受侵犯"之规定属于无法律保留的基本权利,其中就包括隐私权。〔173〕这一宪法上的一般人格权对接民法上的一般人格权,其共同目的旨在对未列举的人格权进行保护。正如学者所说,"民法典规定一般人格权是民事立法者落实基本权利国家保护义务的结果""它乃是一个接收器,处理具体人格权无法保护的领域"。〔174〕伴随着信息技术造成的威胁不断变化,一般人格权势将成为我国信息隐私权未来演化的王牌条款。而保持一般人格权在宪法与民法上通道的对接性,其核心意义就在于宪法条款对立法机关所具有的约束力。〔175〕正如研究者所言,我国宪法从来没有成为单纯约束国家权力的基本法,私人权力始终在制宪者视野之中;基本权利的国家保护义务功能乃是我国宪法的题中之义。〔176〕这一点为同时制约公私信息权力提供了宪法上的重要依据。

我国信息隐私保护存在民法至上、安全至上和管理至上三大问题,而这三种倾向又都与宪法思维的偏颇有关。主流民法学者认为,虽然域外国家与地区普遍把信息隐私权视为宪法权利,但在我国,由于宪法实施监督制度不完善,因此首先应当将其视为一项民事权利,通过民事立法来保护。〔177〕但事实上,隐私民法保护路径的效果在世界范围都差强人意。〔178〕因为,民法路径将隐私保护的力量完全寄托于法院,信息隐私的执行倚赖于个人,且只能发生于私主体之间,这无法回应新技术发展带来的挑战。实际上,信息隐私宪法化不等同于把信息隐私权写入宪法,也不以宪法司法化为必然前提。宪法化提供的是法律体系重构的基础,最终形成以行政法责任为主,同时辅以民事、刑事等多种责任体系在内的权利树—法律树架构。宪法化在个人权利机制之外,通过算法公开、市场激励、机构监督、风险评估、专家委员会、公共参与等手段,将信息权力主体纳入综合治理的轨道。〔179〕

现行立法还存在安全至上的思维,国家或公共安全成为信息立法的核心保障目标,个人信息保护则降格为维护安全的手段。〔180〕在明确信息隐私权基本权利地位的基础上,立法者应

〔172〕目前,来自德国的基本权利客观价值秩序理论已获得我国学界普遍认同,并被作为理论前提运用于基本权利第三人效力、宪法和部门法的关系,以及具体基本权利问题的分析中。客观价值秩序理论已经成为我国基本权利理论的一部分。参见李海平:"基本权利客观价值秩序理论的反思与重构",《中外法学》2020年第4期,第1063页。

〔173〕参见胡锦光、韩大元:《中国宪法》,法律出版社2007年版,第280页。

〔174〕王锴:"论宪法上的一般人格权及其对民法的影响",《中国法学》2017年第3期,第102—103页。

〔175〕同上注,第121页。

〔176〕国家有义务保护个别公民的基本权利防止来自其他私人的侵犯,国家应当采取适当的措施来避免法益损害。参见陈征:"基本权利的国家保护义务功能",《法学研究》2008年第1期,第52页。

〔177〕王利明,见前注〔2〕,第62—72页。

〔178〕See Neil Richards, "The Limits of Tort Privacy", *Journal of Telecommanications and High Technology Law* Vol.9, 2011, pp.357—384;张新宝:"《民法总则》个人信息保护条文研究",《中外法学》2019年第1期,第72—73页。

〔179〕在实体法之外,基本权利同样是组织法和程序法形成、解释与适用的准则和标尺。See Vgl.Sachs, Grundgesetz Kommentar, München: Verlag C.H.Beck, 1999, S.89,转引自赵宏:"主观权利与客观价值——基本权利在德国法中的两种面向",《浙江社会科学》2011年第3期,第44页。

〔180〕参见孙平:"系统构筑个人信息保护立法的基本权利模式",《法学》2016年第4期,第74—75页。

在宪法价值层面厘清信息隐私与公共安全的关系，“分门别类地构筑专门的系统立法，而不是像现在这样含混不清或者厚此薄彼”。[181] 保障公民基本权利应是维护公共安全的终极目的，而不是相反。进言之，在当前的管理至上思维主导下，公权力往往被排除在法律规制的范围之外，信息隐私保护往往蜕变为网络信息管理手段。在实践中，偏狭的管理思维也可能陷入监管俘虏，形成公私权力合谋和滥用的可能。在自上而下的管理之外，更迫切的是通过自下而上的媒体报道、丑闻公开、舆论监督、公益诉讼，有效限制公私信息权力的过度扩张。

笔者认为，应以正在制定的《个人信息保护法》为契机，连接业已颁布的民法典、刑法及其它法规定，通过法院实践、行政监管和商业治理，为信息隐私搭建一个多管齐下、动态保护、多方参与、激励相容，具有弹性与外接性的宪制体系。这需要打破画地为牢的部门法思维，横跨私法、公法、国内法和国际法，集合各法科智慧，构筑一个既有效保护个人信息，又充分维护信息自由、发展数据经济的隐私体系。[182] 信息隐私权的宪法时刻，任重而道远。

Abstract: The traditional normative foundation of the right to information privacy is based on individualism, taking private and public as the dichotomy, centering on the dimensions of space, things, and subjects, forming five theoretical explanations and six conceptual cores. The Lockian paradigm and Kantian paradigm of privacy have recently converged into the control paradigm, which has become the core principle of contemporary information privacy protection. The intelligent society, especially the big data technology, dismantles the control paradigm's technical assumptions, forming a comprehensive impact, and challenging the normative foundation of information privacy. Technological developments have reconstructed the social landscape, causing a profound dilemma of privacy protection in the dimensions of space, time, and society. It is necessary to re-conceptualize privacy from the perspectives of information theory as well as social theory, and to reconstruct the normative basis of information privacy rights: from individual to social standards; from control paradigm to trust paradigm; from monopoly to communication; from dual confrontation to unity and pluralism; from the perspective of rights to the standpoint of power; from conceptual arbitrariness to pragmatic negotiation. Finally, under the constitutional moment's imminence, this article discusses a new system framework for the future development of China's information privacy law.

Key Words: Right to Informational Privacy; Normative Foundation; System Reconstruction; Big Data Technology; Constitutional Moment

（责任编辑：彭 錞）

〔181〕 同上注，第 76 页。

〔182〕 宪法化机制仰赖大量社会中间组织和多层次制度结构的发育，市场机制是其中的关键力量。有研究者已注意到经济激励对解决个人信息保护与数据经济发展二元难题的重要性。经济激励本质上是为企业和用户就个人信息处理提供对话协商平台。通过生成新的自发制度空间，推动零和博弈走向合作博弈。参见蔡培如、王锡锌：“论个人信息保护中的人格保护与经济激励机制”，《比较法研究》2020 年第 1 期，第 106－119 页。