交大法学 SJTU Law Review
No. 1 (2019)

# 数据隐私问题的维度扩展与议题转换：法律经济学视角

戴　昕*

目次



**摘要**　“数据隐私问题”泛指由公共和商业机构处理个人信息的实践而引发的各类政治、经济、法律和伦理问题。法学界对数据隐私问题的关注仍聚焦于如何建构“个人信息权”这一教义学议题，但互联网经济和数据技术的飞速发展，已使数据隐私问题在个体权益、企业竞争和生产关系三个维度上全面展开。鉴于个体权利建构议题本身有限的智识和实用价值，法学界应尽快转向思考与数据合约监管、数据风险管理、数据资源交易和数据劳务定价等相关的机制设计问题，方能为人类社会寻求回应数据隐私挑战的努力做出有意义的贡献。

**关键词**　数据隐私问题　个人信息　竞争　生产关系　机制设计

当代语境中，“数据隐私问题”(data privacy problems)可宽泛指称由公共和商业机构运用信息数据技术收集、存储、传输、分析个人信息(personal information)的实践而引发的各类政治、经济、法律乃至伦理问题。〔1〕近年来，中国法学界对数据隐私问题给予了高度关注，而常见的研究和探讨集中在如何规范表述、论证个人信息的法律权利性质，并进而在立法上建构“个人信息权”这一教义学议题之上。〔2〕

* 中国海洋大学法学院教授、法学博士。作者曾就本文内容在台湾地区中研院法律学所(2016年)和厦门大学法学院(2018年)作专题报告，感谢两次报告听众的评论和建议。本文相关研究工作获国家社会科学基金一般项目(16BFX015)及中央高校基本科研业务费资助。文责自负。

〔1〕 更为宽泛的提法是“信息隐私”(information privacy)，这一概念除了包含较为现代的数据隐私问题之外，还包含更传统的隐私问题。例如，参见 Paul Schwartz & Daniel Solove, *Information Privacy Law* 2 - 3 (5 ED. 2015); Neil M. Richards & Jonathan H. King, “Big Data Ethics”, 49 Wake Forest L. Rev. 393, 395 (2014)。

〔2〕 参见张莉：《个人信息权的法哲学论纲》，载《河北法学》2010年第2期；王利明：《论个人信息权在人格权法中的地位》，载《苏州大学学报》2012年第6期；王利明：《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》，载《现代法学》2013年第4期；叶名怡：《论个人信息权的基本范畴》，载《清华法学》2018年第5期。

2017年《民法总则》通过时，在第111条中规定“自然人的个人信息受法律保护”，但并未如之前学界和实务界期待的那样，给出“个人信息权”这一明确说法，[3]一锤定音地完成对这种区别于传统民事隐私权的新型法律权利的建构。虽然一时“受挫”，但由于立法确权被各界视为应对中国互联网经济发展催生的日益严峻的数据隐私问题的关键，因此可以预见，个人权利建构作为一项学术和制度课题，在私法（如民法）和公法（如个人信息保护法等）两条战线上，都将是法律人持续着力的重点。[4]

在形式层面尽可能完善地建构个人信息权或类似的个体权利，当然有其制度价值。但从法律经济学视角切入，[5]借助理论梳理和分析，本文旨在提示，数据隐私领域中值得法学界在当下和未来关注、思索、讨论的，远不止如何建构、保护个体权利这一表层议题，而学界对数据隐私问题的理解也亟待更新和深化。伴随着互联网经济和数据科技的迅速发展，数据隐私问题在近二十年来不断向更深层次、更复杂化的利害关系维度扩展。即使在最表层的个体权益维度，为切实兼顾、平衡个体利益与社会福利，学界和实务界也应清醒地认识到赋予、保障个体享有选择权和控制权这一思路的局限性。而在以个人信息作为主要生产资源的互联网新经济中，数据隐私问题已充分扩展至企业竞争维度，与之相关的制度安排对数据经济走向垄断还是保持开放正产生重要影响。更进一步，随着人工智能主导的生产模式的兴起，数据隐私问题也开始深入到生产关系维度，并有可能成为撬动劳资关系结构性重塑的力量。而对于研究者来说，无论是在个体权益、企业竞争还是生产关系维度上，仅围绕建构信息主体个体权利这一议题研究和讨论数据隐私问题，其智识和实用意义的局限性都已越发显现。

基于此，本文提议，法学界和实务界都应尽快将其在数据隐私领域关注、探讨的核心议题，从如何在形式上建构法律权利，转向如何进行更富想象力和实用性的机制设计。只有积极参与与数据合约监管、数据风险管理、数据资源交易和数据劳务定价等事项相关的市场和制度机制设计工作，法律人在回应人类社会所面临的日益复杂、重大的数据隐私问题时，才有可能做出具有实质意义的智识贡献。

## 一、维度扩展：个体权益

从法律经济学视角切入，数据隐私问题的最基础维度涉及围绕个人信息的收集和处理而可能产生的“个体”与“社会”之间的冲突。在此不妨将数据隐私问题的这一维度称为“个体权益”维度。不难想见，传统数据隐私法研究的视野主要落在这一维度之上，而研究者应对这一维度数据隐私问题的主要思路，则是寄望通过妥善界定个体权利来平衡个体偏好与社会福利之间的潜在矛盾。与此相比，不同时期的法律经济学研究基于不同理由揭示，如果数据隐私制度的目标是最大化社会总体福利，那么以信息主体的个体控制为基础建构法律权利，未必能够有效地促进这一制度目标。

波斯纳（Posner）、斯蒂格勒（Stigler）和赫什莱弗（Hirshleifer）等学者在早期借助信息经济学理论讨论隐私保护时均认为，保护隐私的法律制度并不符合经济效率的要求。这是因为，正如商业交易中一方不应向另一方隐瞒有可能影响后者决策的重要信息，更广泛意义上的人际交往中，双方信息不对称也会妨碍人们在充分信息的前提下自愿做出有效率的选择，导致机会主义行动

〔3〕 参见张玉学：《专家：讨论中的民法总则草案增加了“个人信息权”》，载《财经》杂志，2016年9月21日。

〔4〕 继续推进个人信息保护专门立法的主张，参见周汉华：《探索激励相容的个人数据治理之道》，载《法学研究》2018年第2期，第14～16页。

〔5〕 本文所谓“法律经济学视角”，所指为广义的经济分析，既包含微观福利分析，又涉及相对宏观的政治经济结构分析。

（如欺诈）的空间出现，并破坏个体投资有价值人力资本的激励。〔6〕在这个意义上，个体基于隐私理由拒绝披露个人信息的行为甚至曾被称为“社交欺诈”，〔7〕而这一说法显然意味着论者对隐私保护的效率意义持否定态度。

但这类早期观点显然过于极端（尽管论者应是有意如此）。后续研究指出，在经济学意义上，保护隐私可以具有正面效率意义。首先，如果将个体对独处、自主、尊严等主观价值的偏好〔8〕也明确纳入社会总体福利——或效率——的考量之中，那么个体就保持本人信息私密、安全获得的效用，未必一定低于相同信息在未获本人同意的情况下被他人获取并利用所产生的价值。因此，保护隐私，正如保护财产权，可以避免无效率的非自愿信息收集和使用过多发生。〔9〕

第二，与其他侵权损害类似，数据隐私问题也可被理解为负外部性问题，或“社会成本”问题。在现代语境中，政府和企业大规模收集、存储和利用个人信息的行为，被赫希（Hirsch）等论者与工业生产造成的环境污染类比：〔10〕收集、处理、使用个人信息的过程制造了包括个人信息泄露、滥用在内的风险和损害，如同废气废水；而相关社会成本除了包括由具体的信息主体承受的损害外，如本-沙哈尔（Ben-Shahar）提示，还可能包括更为抽象的公众损害。例如，当社交网站用户的个人信息被数据公司获取以用于干扰、操纵选举时，社交网站收集、聚集并授权他方使用大量用户数据行为的负外部性，就包括更为抽象、难以计量的民主制度本身的崩坏。〔11〕负外部性或社会成本问题的存在，意味着即使只从经济效率的角度展开论证，对个人信息不予任何保护、任由其被自由获取和传播，也不可能是最优的制度安排。

第三，另有更进一步的讨论指出，数据隐私保护水平过低之所以缺乏经济效率，还应从有价值个人信息生产的角度去理解。众所周知，数据隐私问题在现代社会之所以获得空前重视，不仅因为个人信息的收集、传播和使用对信息主体本身的人格和物质利益有直接影响，还因为对个人信息的有效利用是互联网新经济创造价值的基本方式。在这一前提下，Cofone 指出，有价值的个人信息，具有接近公共品（public good）的属性——被生产出来之后，边际上的传播和使用成本极低，但其生产本身却并非无成本，因此理性的个体只有在其披露数据的私人边际收益（如使用网站提供的服务）超出边际成本（如因个人信息披露而遭受隐私泄露、身份盗窃或价格歧视等损害）时，才

〔6〕 Richard A. Posner, “The Right of Privacy”, 12 Ga. L. Rev. 393, 394 - 403 (1978); Richard A. Posner, “Privacy, Secrecy, and Reputation”, 28 Buff. L. Rev. 1, 7 - 24 (1979); Richard A. Posner, “The Economics of Privacy”, 71 Am. Econ. Rev. 405, 405 - 409 (1981); George J. Stigler, “An Introduction to Privacy in Economics and Politics”, 9 J. Legal Stud. 623, 629 - 631 (1980); Jack Hirshleifer, “Privacy: Its Origin, Function, and Future”, 9 J. Legal Stud. 649, 649 (1980).

〔7〕 Posner, “The Right of Privacy”, *supra* note〔6〕, at 394 - 403.

〔8〕 Cathy Goodwin, “A Conceptualization of Motives to Seek Privacy for Nondeviant Consumption”, 1 J. Consumer Psychol. 261 (1992).

〔9〕 Richard Murphy, “Property Rights in Personal Information: An Economic Defense of Privacy”, 84 Geo. L. J. 2381, 2382 (1995).

〔10〕 Dennis Hirsch, “Protecting the Inner Environment: What Privacy Regulation Can Learn From Environmental Law”, 41 Ga. L. Rev. 1, 23 (2006); James P. Nehf, “Recognizing the Societal Value in Information Privacy”, 78 Wash. L. Rev. 1, 74 - 81 (2003). Omri Ben-Shahar, “Data Pollution”, University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 854; U of Chicago, Public Law Working Paper No. 679, Jun. 2017, *available at* SSRN: https://ssrn.com/abstract=3191231, last visited 2018 - 12 - 02. 此外，从第三方外部性的角度对政府行为（如刑事侦查）造成的隐私侵害所做的分析，见 Orin S. Kerr, “An Economic Understanding of Search and Seizure Law”, 164 U. Penn. L. Rev. 591 (2016)。

〔11〕 Ben-Shahar, *supra* note〔10〕, at 4.

会选择参与信息生产。[12] 如果没有合理的个人信息保护制度，网络用户完全可能因为担心披露高价值个人信息对自身造成过度不利的影响，而减少使用服务，不披露、少披露数据，[13]从而导致信息生产总体规模低于最优水平。

尽管上述三类论证角度不同，但都支持保护个人信息具有经济效率的结论。而在这个意义上，法学界倡导的以个体权利建构应对数据隐私问题的制度方案，看来能够获得初步的经济学证立：如果法律对个体针对其个人信息所享有的各类权益进行界定和确认，并在此基础上赋予、保障信息主体自身的选择权和控制权，使得相关信息的收集、传播、使用都获得信息主体的知情同意，那么自愿交易就可以实现有价值个人信息的有效率配置，而外部性等问题也可通过交易或模拟交易的赔偿机制得到化解。

然而进一步的研究很快指出，即使赋予并保护个体选择权与控制权，个体权益维度的数据隐私问题也不可能像前述科斯式逻辑所推论的那样迎刃而解。首先，如果接受传统经济学理论有关信息主体理性的假设，那么鉴于广大消费者在现实中普遍大量、随意地向商家披露其个人数据的情况，有理由怀疑，个体有关数据隐私的偏好，或许没有隐私法学者理解得那样强烈；而数据经济对个体的情感健康、个体尊严乃至物质福利等所造成的实际损害，也没有学者常常假想的那样严重。[14] 换言之，即便数据隐私问题真的意味着沉重社会成本存在，那么这些社会成本可能主要也不体现在每个信息主体都有动力直接寻求维权的私利，而是体现在每个人虽在抽象意义上都受影响、但却很难进入具体个人私利决策的系统性问题，如因数据滥用导致的选举操控、国防情报泄露、消费金融体系欺诈风险增加、弱势群体受歧视增加等。[15] 即使法律清晰地建构出每个个体享有的权利，这类更抽象的外部性问题也很难靠个体选择和控制而获得内在化。

其次，仍以个体理性为前提，在大数据语境中，由于意识到数据收集和使用无所不在，个体信息主体即使被赋予受保护的选择权和控制权，他们仍有可能基于策略性动机而选择过度披露。例如，当金融、保险或零售等行业的经营者用更优惠的服务条款为诱饵，鼓励消费者披露包括收入、个体健康状况或行为习惯等个人信息时，消费者会担心，如果其拒绝披露，商家会据此采取对其不利的价格歧视；类似地，当雇主鼓励求职者自愿披露个人信息时，求职者也会担心保持沉默会导致雇主对其个人情况的负面推论。因此，Peppet等指出，这种考虑及由此产生的压力，会使得信息主体进入自我披露的军备竞赛。[16] 此时，信息主体的披露行为即使是“自愿”选择的结果，却不但未

---

〔12〕 Ignacio N. Cofone, “The Dynamic Effect of Information Privacy Law”, 18 Minn. J. L. Sci. & Tech. 517, 538 (2017).

〔13〕 Cofone, id. at 540－541. 这一情况在社交网站领域已经广为人知。例如，参见《那些消失在朋友圈里的中年男人》，载搜狐网2018年10月6日(https://www.sohu.com/a/257899128_682886，最后访问时间2018－12－02)。

〔14〕 这是对著名的“隐私悖论”(privacy paradox)的一种解释。*See* Alessandro Acquisti, Leslie K. John & George Loewenstein, “What is Privacy Worth?” 42 J. Legal Stud. 249 (2013).

〔15〕 *See* Ben-Shahar, *supra* note〔10〕, at 9－12.

〔16〕 *See* Scott R. Peppet, “Unraveling Privacy: The Personal Prospectus and the Threat of A Full-Disclosure Future”, 105 Nw. U. L. Rev. 1153 (2011); Mark MacCarthy, “New Directions in Privacy: Disclosure, Unfairness and Externalities”, 6 ISJLP 425 (2010－2011). *See also* David Dranove & Ginger Zhe Jin, “Quality Disclosure and Certification: Theory and Practice”, NBER Working Paper No. 15644, 2010, *available at* http://ssrn.com/abstract=1537763 (last visited 2018－12－02). 一些提供消费者生理数据监控设备的公司已经开始寻求与保险公司合作的营收模式。Scott R. Peppet, “Privacy & the Personal Prospectus: Should We Introduce Privacy Agents or Regulate Privacy Intermediaries?” 97 Iowa L. Rev. 77, 91 (2012). *See also* Alice E. Marwick, “How Your Data Are Being Deeply Mined”, N.Y. Rev. Books, Jan. 9, 2014, *available at* http://www.nybooks.com/articles/archives/2014/jan/09/how-your-data-are-being-deeply-mined/ (last visited 2015/07/23).

必符合自身效用和偏好，而且也可能导致第三方信息遭受无效率的非自愿披露。〔17〕

第三，由于个体信息主体会基于理性和非理性的因素，同时面临认知和决策方面的局限，因此在现实中我们不能将实现个人信息有效生产、有效配置的期望寄托在信息主体的自主选择之上。对于当代互联网经济中较为复杂的商业行为和交易安排，例如数据挖掘和网站隐私政策等，消费者个体即使在获得充分信息披露的情况下，也常常难以准确理解、想象其内容和后果。〔18〕在这个意义上，数据隐私或安全对于普通网络用户来说是“信用物”（credence good），人们在消费前或消费后均很难确定，其应为某种水平的个人信息保护支付多高代价。〔19〕而如果我们将行为经济学关于有限理性和有限意志力的洞见纳入考量，那就更不难想见，受有限意志力的影响，就选择是否进行信息披露或相关授权而言，个体往往会更关注从商家获得服务或优惠的近期收益，却对信息披露可能产生的远期成本缺乏考量；不仅如此，现实中对消费者隐私决策实际产生影响的，往往是网站界面呈现、设计以及缺省规则等商家有能力也有动力予以操控的因素。〔20〕

需要说明的是，与其他许多领域类似，在数据隐私问题上强调个体选择和自愿交易虽然不足以保证社会福利最大化，但不意味着法律制度不应赋予并保障信息主体在一定程度上享有选择权与控制权。这一部分重点在于揭示，即使只为应对个体权益维度上的数据隐私问题，当下学界投入较大精力试图完成的个体法权——特别是私法上的个人权利——建构，本身也具有严重的局限性，远非对实质性问题做出的充分制度回应。

而另一方面，尽管“名正言顺”的“个人信息权”在中国尚未落在白纸黑字上，但《侵权责任法》《刑法》《网络安全法》及一系列其他法律、行政法规、部门规章、地方性法规、司法解释等，当下已然从各角度寻求保护公民作为信息主体的个体权益。〔21〕仅就已有的规范内容来说，我国对信息收集、处理的主体同意要求，甚至已经比其他国家要来得更为严格。〔22〕在这一前提下，“个人信息权”或类似个体权利是否要获得独立、明文的立法界定，相比于落实执行上述既有的各类相关制度规范，对于实现信息主体选择权和控制权而言，其实际意义就显得有限。这更使人怀疑，学界如在当下和未来仍以形式化权利建构为主要研究和鼓呼的议题，能否收获足够的产出。

## 二、维度扩展：企业竞争

数据隐私问题在当前社会经济条件下已呈现出的第二个维度，可称为“企业竞争维度”。企业竞争维度的数据隐私问题在一定程度上是个体权益维度上相关问题的延展。而看到数据隐私问题对互联网新经济结构中企业竞争的潜在影响，有助于我们更清晰地意识到形式化权利建构思路的局限性。

在当代信息经济语境中，数据隐私问题因个人信息作为生产性资源的属性，而与经济价值生

---

〔17〕 参见戴昕：《自愿披露隐私的规制》，载《法律和社会科学》2016年第15卷第1辑，第24～27页。

〔18〕 Ignacio N. Cofone & Adriana Z. Robertson, “Consumer Privacy in A Behavioral World”, 69 Hastings L. J. 1471, 1491－1497 (2018).

〔19〕 Ben-Shahar, *supra* note〔10〕, at 20.

〔20〕 *See generally* Alessandro Acquisti, Laura Brandimarte & George Loewenstein, “Privacy and Human Behavior In the Age of Information”, 347 Science 509 (2015).

〔21〕 如《侵权责任法》、《刑法》、最高人民法院《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》、最高人民法院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（2017）、《网络安全法》（2016年）、《消费者权益保护法》（2013年修订）、《上海市社会信用条例》（2017年）等。

〔22〕 参见高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018年第3期，第8页。

产过程发生了直接、密切的联系。尽管信息主体的自愿披露、授权收集是整个信息生产环节的起始点，但在此基础上，企业对收集到的个人信息所进行的各类加工处理，对于经济价值的产生和提升无疑更为关键。在这一背景之下，实务界曾在一个时期内，纷纷提出了在个人信息权界定的基础上进一步界定“企业数据权”的规范建议。例如，有论者曾提出，立法上应确立“原始数据”和“衍生数据”两类权利客体，〔23〕而另一种说法则提出应区分“基础数据”与“增值数据”。〔24〕在这些论调中，所谓“原始数据”或“基础数据”，指的都是信息主体直接披露的个人信息，而所谓“衍生数据”和“增值数据”，则是在企业对前者进行脱敏、归集、分析等加工处理之后产生。〔25〕在对这两类数据明确划分界限之后，来自实务界的这类论调即主张将“原始数据”或“基础数据”作为“个人信息权”的客体，而“衍生数据”或“增值数据”作为“企业数据权”的客体。

初看之下，“企业数据权”无非是“个人信息权”的反题：既然为了保护个体权益，必须把个人信息权建构、界定清楚，那么凡未被囊括在个人信息权之内的数据资源，便都可由企业自由、灵活地利用，无须因个体权益保护的目的受更多限制。但实际上，除了在个体权益维度协调“个体—企业（社会）”关系之外，“企业数据权”的真正要害在于，这是一种企业针对数据资源提出的排他性专有的主张。不难想见，如果数据是所谓数字经济时代的“石油”，那么对于其投入成本收集个人信息再加工处理而成的各类高价值数据资源——简单到客户名单、用户交易记录，复杂至数据挖掘分析结论和模型等——企业当然有动力尽可能独享与之相关的经济利益。

为了证立有关这一排他性专有权的诉求，企业不出意料地要诉诸“劳动创造产权”的经典财产理论。〔26〕但更有意思的是，保护用户的数据隐私，也常常成为主张排他性权益的企业祭出的重要理论依据。前些年新浪微博和脉脉之间有关用户数据的纠纷是绝佳的示例。作为纠纷产生的背景，脉脉原本与新浪微博之间存在商业合作关系，后者为前者提供数据接口，使得新浪微博用户可以利用新浪微博的账户登录脉脉的职场社交网络平台。但在未获得非脉脉用户的微博用户以及微博平台授权的情况下，脉脉通过抓取微博公开信息的方式，收集了更多微博用户的头像、职业和教育背景等个人信息，用于建设、扩展脉脉平台上的社交网络。新浪微博起诉脉脉，指控后者的行为不但构成不正当竞争，而且侵害了微博用户的隐私和安全。〔27〕而在新浪微博与包括脉脉在内的合作开发者之间所签订的开发者协议中，新浪微博的确明确要求第三方开发者在需要收集微博用户数据时，必须事先获得用户的知情同意。〔28〕

脉脉案以新浪微博胜诉告终。而这场官司因微博采取了依托保护用户隐私的名义维护自身竞争利益的诉讼策略，使得数据隐私问题在企业竞争维度的展开鲜明地跃上了中国信息法治的前台。脉脉因未取得用户同意而明确违反了开发者协议，使得该案的司法处理简单化了。但这不意

〔23〕 参见杨立新、陈小江：《衍生数据是数据专有权的客体》，载中国社会科学网（http://orig.cssn.cn/sf/bwsf_fx/201607/t20160713_3120938.shtml，最后访问时间2018-12-02）。文章刊发时陈小江单位显示为阿里巴巴集团法务部。

〔24〕 参见丁道勤：《基础数据与增值数据的二元划分》，载《财经法学》2017年第2期。文章刊发时丁道勤单位显示为京东集团法务部。

〔25〕 参见前注〔23〕，杨立新、陈小江文；前注〔24〕，丁道勤文。

〔26〕 参见前注〔24〕，丁道勤文，第8～9页。

〔27〕 北京淘友天下技术有限公司等与北京微梦创科网络技术有限公司不正当竞争纠纷二审民事判决书（2016）。

〔28〕 新浪微博当时的开发者协议中规定：“开发者应用或服务需要收集用户数据的，必须事先获得用户的同意，且仅应当收集为应用程序运行及功能实现目的而必要的用户数据和用户在授权网站或开发者应用生成的数据或信息。开发者应当告知用户相关数据收集的目的、范围及使用方式，以保障用户的知情权。”

味着企业竞争维度的数据隐私问题不会变得更为复杂。试想，如果甲企业获取乙企业收集的用户数据，虽未获得乙企业的同意，但却取得了乙企业用户的授权，此时，甲企业的行为是否会构成不正当竞争，或在任何其他意义上侵犯了乙企业的某种权利？尽管此类争议并未进入法院、形成有代表性的判决，但在实践中其实早就出现过。据报道，某些记账类应用，就曾通过要求其注册用户接受一揽子授权式用户协议的方式，使用户授权其可"从任何第三方"收集该用户的个人数据；在此基础上，这类财务应用甚至可以要求用户提供其在另一金融平台（如支付宝）上的账号和密码，进而自行访问该用户在后一类金融平台的账户，从中提取用户的交易记录和其他信息。〔29〕尽管在抽象意义上，记账应用经营者的这类数据获取行为是在用户授权的前提下做出的，但必然遭到金融平台的反对，因为后者认为，记账应用获取的金融平台账户内数据，已不仅仅是个人信息，而是经过金融平台加工处理后的高价值数据资源，或"增值数据"，不再处于其用户基于个人信息权的主张可加以控制的范畴之内。例如，支付宝的用户协议中就明确规定，"支付宝会员号和账户仅限您本人使用，不可转让、借用、赠与、继承"。〔30〕

实际上，"账户"并非一个空壳，而应被理解为包含了各类用户个人信息的一个信息权益集合。但上述用户协议实际上通过合同的方式，切断了信息主体与账户信息之间的联系，为企业通过技术排斥手段——如为其他企业使用用户账号密码登录平台获取数据的行为设置技术障碍——已然在为谋求实现的排他性数据权利提供进一步的保障。由此看来，借用劳伦斯·莱斯格（Lawrence Lessig）的概念框架，〔31〕为了支持自身对其在用户个人信息之上处理获得的数据资源享有独占权益，互联网企业在技术、市场（合同）和规范（创造权利话语）这几个角度都已有所着力，就差法律对"企业数据权"的概念加以确认这一锤定音了。而事实上，《民法总则》草案中也确实曾酝酿过"数据信息"被纳入知识产权客体范畴的方案，〔32〕只是到最终稿才放弃这一思路。〔33〕

正是透过此类有关"企业数据权"的主张和相关争议，我们才更清晰地看到，在企业竞争维度，数据隐私问题的真正面向，并非用户个体的权益受到何种侵害、应如何加以保护——尽管涉及数据争议的企业仍大张旗鼓地要将用户隐私带入讨论，甚至将保护数据隐私作为支持其排他性竞争权益的重要理由。而数据隐私问题以类似方式在企业竞争维度展开、呈现，也不是中国特色。在美国2017年一个引人瞩目的司法裁决中，加州北区的联邦地区法院裁定著名职业社交网站LinkedIn无权阻碍猎头数据分析公司hiQ Labs使用爬虫软件爬取LinkedIn网站中用户"公开"的个人信息。与新浪微博案中的原告类似，LinkedIn在此案中指出hiQ Labs爬取用户个人信息的行为对用户的隐私和信息安全构成了威胁。〔34〕但主审法官在裁定时支持hiQ Labs商业模式和数据获取行为的合法性，不但指出LinkedIn保护用户隐私的主张是虚伪的——与其自身以大量收集、分析个人信息为依托的商业模式形成鲜明反差——，甚至暗示LinkedIn对hiQ Labs的压制有

〔29〕 对此类企业曾经采取的相关实践的一个详细描述，参见知乎（https：//www.zhihu.com/question/24918809/answer/47549119，最后访问时间2018－12－02）。其中涉及相关企业的用户协议经查已修改。

〔30〕《支付宝服务协议》四（二）3（https：//render.alipay.com/p/f/fd-iztow1fi/index.html，最后访问时间2018－12－02）。其他公司也均采用类似的账号规则。参见岳林：《网络账号与财产规则？》，载《法律和社会科学》2016年第15卷第1辑，第54～56页。

〔31〕 Lawrence Lessig, "Code: And Other Laws of Cyberspace", Version 2.0 86－95 (2006).

〔32〕《解析民法总则草案首次明确网络虚拟财产物权》，载人大新闻网2016年7月19日（http：//npc.people.com.cn/n1/2016/0719/c14576－28567076.html，最后访问时间2018－12－02）。

〔33〕 正式颁布的《民法总则》第127条仅规定，"法律对数据、网络虚拟财产的保护有规定的，依照其规定"。

〔34〕 *hiQ Labs, Inc. v. LinkedIn*, 2017 WL 3473663 (N.D. Cal. Aug. 14, 2017).

可能违反了反垄断法。[35] 这一裁决与此前美国一些涉及数据爬取的判例取向相左，令观察者大跌眼镜。[36] 但这也体现出美国司法界至少有部分人士对“开放互联网”(open internet)的理念颇为买账，对企业数据权主张的反竞争意涵则高度警惕，即使这种企业独占权的主张会被用保护用户个人隐私的理据包装起来。

而相比于hiQ Labs案的初审裁决，更激进的抵制企业数据排他专有的立场，则体现在欧洲已经通过的《通用数据保护条例》(GDPR)正式确立的数据可携权(portability)制度。可携权制度意味着用户对其授权提供给企业的个人信息享有持续延伸的控制权：在这种制度下，用户更换网络信息服务商时，可要求将其在现服务商处保存的个人信息直接迁移到新的服务商。[37] 而根据2017年欧盟工作组就可携权条款出具的进一步指导意见，用户可要求服务商迁移的信息范围，明确包括用户在现有服务商平台上积累的、被直接观察到的活动历史和他人评价(尽管不包括进一步的综合评分)等。[38] 不难想见，对于积累巨大用户资源的成熟互联网企业来说，可携权一旦落实，将会对其排他专有数据资源的诉求构成冲击。而将降低竞争门槛的钥匙交给个体用户，则再次印证了数据隐私问题在现实中已经超出个体权益维度。然而值得疑问的是，可携权这一围绕个体选择建构的权利，真是实现数据资源最优配置的权益安排模式吗？至少，在有效落实可携权的技术和市场机制形成并获得广泛应用之前，[39]我们对于这一试图借助个人控制权有效撬动竞争的思路，只能暂且保持观望。

## 三、维度扩展：生产关系

随着人工智能的研究和应用近年来迅速发展，数据隐私问题正进一步延伸到更为宏观、也更具基础意义的生产力如何发展、生产关系如何安排这一政治经济学维度。而数据隐私问题出现这一扩展的主要原因在于，人工智能在当下和近期的继续发展，仍以获取高质量数据作为基本前提。

关于人工智能在宏观上可能对人类社会现有政治经济安排带来的冲击和挑战，业界、学界和民间早有各类推测和构想。由于人工智能已开始逐步在越来越多的领域替代人类劳动力的作用，[40]根据某些末日论调，人类最终将完全被机器取代，甚至像主奴辩证法所提示的那样，最终被机器或机器背后的极权资本所奴役。[41] 即使不那么科幻，根据芝加哥大学的两位经济学家基于1975年至2012年间59个国家的数据做出的观察和分析，与人类近代历史以往有关技术革命的经验不同，自20世纪80年代以来，基于信息科技的发展，人类劳动者收入在社会总体收入中所占的

---

〔35〕 *Id*. at 23.

〔36〕 Venkat Balasubramani, “LinkedIn Enjoined From Blocking Scraper-hiQ v. LinkedIn”, Technology & Marketing Law Blog, August 15, 2017 (https://blog.ericgoldman.org/archives/2017/08/linkedin-enjoined-from-blocking-scraper-hiq-v-linkedin.htm, last visited 2018-12-02).

〔37〕 EU General Data Protection Regulation, Art. 20.

〔38〕 Guidelines on the Right to Data Portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01, pp.9-10.

〔39〕 见下文第四部分第3节。

〔40〕 有预测指出，未来数十年中，人工智能将使50%的工作岗位实现自动化。Carl Benedikt Frey & Michael A. Osborne, “The Future of Employment: How Susceptible are Jobs to Computerisation?” 114 Technological Forecasting & Social Change 254 (2017).

〔41〕 例如，孙大剩：《〈西部世界〉中的主奴辩证法》，载澎湃新闻2016年12月13日(https://www.thepaper.cn/newsDetail_forward_1578937，最后访问时间2018-12-02)。

比重，不再如以往那样能够维持在技术革命之前的水平，而是出现了非常明显的下降。〔42〕这一趋势更为真切地提示，随着人工智能生产力的提高，人类劳动确实可能进一步、甚至彻底失去其在传统意义上的生产价值。

如果大趋势如此，那么人类社会在未来面临的一项重要挑战，看来就是重新建构与财富分配有关的基本社会契约。而假设人工智能真的全面取代人类劳动，那么后者也就无法再成为人类个体主体性和价值尊严的来源，人之为人的依据甚至因此要转向“闲暇”(pleasure)或“游戏”(play)，而个体生活的基本保障也只能依靠类似“普遍基本收入”(Universal Basic Income)这样在历史和现实中已经被提出并在一些国家以不同形式施行的政府财政措施。〔43〕

但正如 Arrieta-Ibarra 等学者所提出的，在多种未来可能中，这应该只是其中一种；与之相比，应还有更有利于维护人类主体性和劳动价值的生产关系安排方案。〔44〕而这种预测的核心逻辑前提就在于，人类个体通过生产数据参与机器学习，至少在当前和未来一定时期内，仍会是人工智能介入乃至趋于主导的生产模式所必须包含并倚重的基本生产环节。尽管人工智能已被渲染得神乎其神，但截至目前，无论是早期基于编程的人工智能，还是新一代基于机器学习的人工智能，其对社会生产力提高的贡献都较为有限；究其原因，特别是对于机器学习来说，充足规模的高质量数据是开发出真正有生产价值的算法所必需的资料，而此类高质量数据在“免费数据换免费服务”的互联网商业模式下供给不足：尽管消费者自愿提供并为各类数据企业获取的个人行为数据规模极为庞大，但这类数据总体上都以消费而非以生产为导向。〔45〕例如普通网络用户浏览电商网站页面的踪迹这一类数据，对于企业来说收集成本极低，也构成了所谓“大数据”中最常见的类别；相比之下，有关人类如何对不同语文进行翻译、律师如何对合同条款进行审阅等行为的样本数据，收集难度就要大得多。〔46〕如果机器学习主要只能以免费互联网所生产的消费导向的信息为原料，那么包括神经网络在内的各类算法，只能“学习”到人类消费行为的特征，却无法借助有效的范例模拟人类的生产、创造活动——尽管后者才是人们真正寄望人工智能获得广泛应用，且对由此可能带来的影响感到担忧的领域。

因此，人工智能的发展，看来正面临一个与数据隐私问题有关的微妙困局：尽管从总体趋势上看，人工智能有望驱动生产力大幅飞跃，并由此带来生产关系的剧烈变动，但在这一切发生之前，人工智能生产潜能的充分开发，本身却受到生产导向数据不足这一瓶颈的严重局限。而为了促使更多生产导向数据获得生产、满足人工智能开发的需求，恐怕又正需要从数据隐私问题着手，先行展开生产关系的重构。据此，有学者提出，既然数据对于人工智能生产过程来说应被视为生产资料，那么个人作为信息主体所从事的一切产生数据的活动，本身就可被定义为劳动，而人工智能企业从信息主体处收集信息的过程，则应被视为由劳动者参与人工智能生产过程的一个基本劳动环

---

〔42〕 Loukas Karabarbounis & Brent Neiman, “The Global Decline of the Labor Share”, 129 Quarterly J. Econ. 61 (2014).

〔43〕 Parijs, Philippe Van and Yannick Vanderborght, *Basic Income: A Radical Proposal for A Free Society and A Sane Economy* (Havard University Press, 2017), pp.70 - 98.

〔44〕 Imanol Arrieta-Ibarra, Leonard Goff, Diego Jimenez Hernandez, Jaron Lanier & E. Glen Weyl, “Should We Treat Data as Labor? Moving Beyond ‘Free’”, 1 Am. Econ. Assoc. Papers & Proceedings 1 (2018).

〔45〕 *Id.* at 1 - 2; Eric Posner & E. Glen Weyl, *Radical Markets: Uprooting Capitalism and Democracy for A Just Society* (Princeton University Press, 2018), Ch.5.

〔46〕 以 2018 年发布的著名的法律人工智能实验为例，研究者为开发可实现简单合同审阅任务的人工智能算法，聘请了 20 位业内资深律师参加，提供机器学习的样本数据，其成本可想而知。Comparing the Performance of Artificial Intelligence to Human Lawyers in the Review of Standard Business Contracts, Lawgeeks, Feb. 2018 (https://images.law.com/contrib/content/uploads/documents/397/5408/lawgeex.pdf, last visited 2018 - 12 - 02).

节，而企业理应就数据生产向劳动者支付报酬。〔47〕

这种被相关学者称为“数据作为劳动”（data as labor，或“DaL”）的新型数据生产关系模式，其对应的是传统商业互联网中用户数据因用户使用服务而被企业免费收集、并由此形成企业投资成果和专有资源的“数据作为资本”（data as capital，或“DaC”）模式。鼓吹者认为，DaL相对于DaC的优势在于，一方面，信息主体在体现DaL的数据权益安排之下，将会有更充足的动力进行生产导向的高价值数据生产——而这与个人权益维度上有关数据隐私保护制度效率意义的论证形成勾连；另一方面，在DaL模式下，政治经济学关注的劳动者地位和人类主体性问题，出现了新的想象空间，即人类作为信息主体所从事的各项活动，在其生产高价值数据的意义上，仍可被界定为劳动，而人类劳动者也因此将继续因数据劳动而享有主体性、尊严——当然，还有劳动报酬。〔48〕

尽管DaL是学者在宏观政治经济学层面提出的人与数据、人与人工智能关系的构想，但这一构想又对思考个体权益和企业竞争两个维度上的数据隐私问题给出了方向性的提示：如果数据生产本身应被视为劳动，那么信息主体对于本人信息的控制，就可类比于其对于自身劳动力和劳动成果的控制，而企业对于其获取的数据所享有的专有权，也至多不应超出企业对传统劳动力和人力资源所享有的专有权限度，且数据资源的流动和共享利用应在尽可能的范围内获得鼓励和保障。

但需要注意的是，如果我们将落实DaL这一数据生产关系的安排，仅仅寄托于赋予个体数据劳动者以个体信息控制权，那么数据隐私问题无疑就又会再次循环、落回到其在个体权益维度所面临的相同困境：由于广大网络用户在免费互联网模式常年浸淫下，已经产生了路径依赖，又不了解、也无法了解机器学习背景下自身参与数据和人工智能生产的意义，并且大型数据企业也有激励借助其买方垄断地位（monopsony）维持现有的用户认知和行为习惯，〔49〕因此以建构、赋予个体权利为核心面向的法律制度，实际上无法保证数据不继续被资本以较低的对价收割。不仅如此，还需要看到，如果DaL模式的证立依据是因其更有助于人工智能提高生产力这一潜能的充分兑现，那么此处暗含的一个基本要求，就是市场——或某种类似、模拟市场的机制——能够基于实际被生产出来的数据的质量，对不同的数据劳动价值做出区分定价。而就目前来看，对数据劳务实现有效定价的机制尚不完善。

除了上述“劳动-资本”二元关系角度的讨论之外，尽管并非本文讨论的重点，但值得在此提及的是，在政治经济学层面，数据隐私问题在今天还由于数据化公共治理（digitized governance）的普遍化而可能产生更为复杂的体制性后果。与商业互联网走向大数据化的进程几乎平行，政府在当代寻求加强、改善公共治理的过程中，不但长期大量收集公民个人信息，也在日益寻求对各类不断更新、升级的数据和算法能力加以应用，这使得政府积累并不断增加收集的公民个人信息，在公共治理领域中同样形成了极为重要的公共资源。尤其在中国语境中，无论是“互联网＋政务”“智慧城市建设”还是更为庞大的社会信用体系建设，这些数据化公共治理实践的全面铺开，一方面意味着国家与公民之间的关系将面临重新形塑，特别是公民自身的数据生产将更为鲜明地成为社会控制的基本依据，而另一方面，国家与包括企业在内的市场组织之间，在社会控制场域中的互动也将更为紧密，特别是数据企业将可能成为国家落实数据化公共治理所依赖的基础设施建设、维护和运营合作者。“国家-企业-公民/消费者”这三类主体之间，由此会出现更加复杂的互动关系。当数据隐私问题处于这一复杂的政治经济学场域时，单纯的个体权利建构思路就显得极为单薄了。

---

〔47〕 Arietta-Ibarra et al., *supra* note〔44〕; Posner & Weyl, *supra* note〔45〕.

〔48〕 *Ibid*.

〔49〕 *Ibid*.

## 四、论题转向：机制设计

前三部分描述了数据隐私问题在当代如何随互联网信息经济的发展而迅速在三个维度上展开，并不断向纵深推进。而在这一背景下，法学界在思考如何对数据隐私问题做出制度性回应时，其视野不应再过度局限于如何建构形式化的个体权利这一传统议题，有关数据隐私问题的制度性思考亟待迎来主要议题的转向。无论是为平衡个体权益诉求与社会福利、协调企业创新激励和市场竞争需要，还是为更妥善地安排面向未来、符合生产力发展要求的数据生产关系，富有想象力又切实可行的机制设计都将显现出极高的重要性。尽管本文无意、也显然不可能充分论证当前急需被提出并获得落实的机制设计方案，但以下初步讨论，旨在为进一步的研究和实践提示若干可能有价值的推进方向。〔50〕

1. 格式化合约设计及其监管

尽管赋予信息主体有关个人信息的控制，本身并不足以保证个体能够在信息收集、存储、使用、交易和利益分配等事项上做出符合社会效率要求的行为选择，但法律提供基准性界权的一个积极价值，是使得信息主体和信息处理者能较为容易地找到交易起点。但统一法律界权的潜在缺陷，是其常常难以照顾不同交易主体及不同交易和社会交往情境中个体对数据隐私的需求存在差异化。尽管在理论上，零交易成本的世界中人们可以围绕任何法律规则展开科斯式交易，有效率地重新配置资源，但高交易成本、缺乏信息、偏爱现状(status quo bias)等因素，还是可能使得法律即使只意图提供作为交易起点的缺省规则(default rules)，但缺省规则常会变得过于粘滞，成为终局性安排。〔51〕

基于此，除了在各类法律法规中正面表述、界定“个人信息权”之外，一项对治理者而言重要且有意义的工作，应是推动、激励乃至直接参与情境化的用户个人信息格式合同协议条款的设计。格式合同在传统的消费者保护法研究中，常被视为商家借以从消费者群体向自身转移财富的工具，并由于其可能侵害消费者所谓的选择权而“显失公平”。〔52〕但更晚近、思路更务实的研究则指出，格式合同在日益复杂的现代经济、特别是互联网经济中，不但不可避免，而且如正确对待、善加利用，总体上可能更有利于消费者福利的改进。〔53〕对于商家和消费者之间有关个人信息的协议——隐私协议或隐私政策——而言，其中需要包含的条款之丰富和琐碎，是每个理性的消费者在进行日常交易时都不可能付出相应成本加以了解，并与企业进行单独洽商的；一律接受格式条款对于每个个体都必定更有效率。而虽然消费者不可能实际去阅读冗长、复杂的格式合同内容，似乎给了商家通过格式合同限制消费者权利、实施不公平交易条款的机会，但需要注意的是，格式合同的批量化使用，本身可以降低监管者的监管成本——通过有效监管厂商个人信息格式合同的内容，监管者反而可以更低的成本将监管触角延展覆盖到作为相应格式合同适用对象的海量交易。

需要指出的是，如果法律就用户个人信息作统一界权，且界权内容足够细致，这实质上就相当于提供了一套各类市场交易主体均要普遍遵行的格式合同。但如前所述，数据隐私问题是场景化的，人们在不同语境中——例如用户使用的是普通社交网站服务还是成人社交网站服务，是在获

---

〔50〕 除本部分讨论的四个方面的机制设计外，其他已被提出并可能值得考虑的项目，还包括设计可行的对“数据污染”征收的庇古税(Pigovian tax)。*See* Ben-Shahar, *supra* note〔10〕, at 39－43.

〔51〕 Omri Ben-Shahar & John A.E. Pottow, “On the Stickiness of Default Rules”, 33 Fla. St. U. L. Rev. 651 (2006).

〔52〕 Arthur Allen Leff, “Unconscionability and the Code — The Emperor's New Clause”, 115 U. Pa. L. Rev. 485, 485－489 (1967).

〔53〕 Omri Ben-Shahar, “Regulation Through Boilerplate: An Apologia”, 112 Mich. L. Rev. 883 (2014).

取金融服务还是医疗服务，等等[54]——对个人信息收集和使用的偏好也注定不同。因此，有效的个人信息市场上，应存在多元而非单一化的格式合同，而数据隐私立法和监管不但要允许格式合同设计的差异化，还应尽量设法助推这种差异化格式合同的出现。例如，在电商、医疗、金融、云计算等不同领域中规制数据隐私问题时，法律在基础规则层面提出差异化要求，本身就有助于各领域内相互有所区别的格式合同的出现。在这个意义上，甚至有理由认为，尽管流行观点认为欧盟的统一高标准信息规制更有利于保护用户隐私，但美国式的部门立法未必没有优势——特别是在联邦贸易委员会(FTC)日益发挥起统一协调和底线式监管职能的基础上，[55]通过不同部门的差异化立法标准，允许互联网、医疗、金融等不同领域形成各自不同的隐私格式条款，可能是更有效率的。

而法律助推格式合同的差异化，其前景还不止基于交易语境的差异化。在大数据行为和心理分析的基础上，有关数据隐私的法律规则和参照相关法律规则设计的个人信息格式合同条款，都可以追求“因人而异”(personalized)。例如，参照 Porat & Strahilevitz 的建议，由于消费者依据“大五人格”(Big Five Personality)框架得到描述的个人心理特质与其信息隐私偏好呈高度相关，法律可要求互联网信息服务提供者根据消费者的人格特质提供差异化的缺省隐私设置，[56]乃至完整的个人信息格式条款；这可使不同消费者获得的隐私与服务的组合，都能够最大化其个体效用，并促进个人信息的生产。

2. 个人信息安全保险

与公众人物相比，绝大多数人在数据隐私领域最为关注的，并非公共形象维护一类隐私利益，而是因个人信息泄露和滥用而可能导致的人身和财产安全风险。法律界权——特别是民法人格权确权——的一个明显价值，是信息主体可据此通过民事诉讼的机制就此类损害寻求救济。但需要注意的是，即使在集体诉讼机制足够有力的制度语境中，侵权诉讼也往往不是一种好的救济信息安全损害的方式。根据欧美已有的相关诉讼经验，在此类民事诉讼中，原告很难证明其遭受的损失与特定信息泄露之间的因果关系，[57]甚至常常无法证明损害本身存在：当大规模信息泄露发生并获得披露时，对于事件涉及的每一个具体信息主体而言，其可能因此遭受的更具体、形象的损害，往往还没有发生，最多是一个概率事件或不确定事件，而任何国家的法院系统事实上都不善于对概率性损害厘定赔偿方案。[58] 但即使每个个体事实上面临的损害预期可能都不大，由于信息泄露风险往往会涉及大量个体，加总之后的规模又相当可观，如果数据收集者和处理者不被充分追究赔偿责任，就会引发较为严重的道德风险。反过来，如果司法者因缺乏信息或过于热衷保护权利，在仅存在概率性损害的情况下，对数据收集者和处理者施加过重的责任，又可能引发用户一侧的道德风险问题，使得企业面临的诉讼负担过重。

因此，为有效控制、管理个人信息泄露产生的安全风险，仅有民事诉讼救济是不够的，基于系统性风险评估和风险管理的保险市场是合理补偿个体风险损失、满足个体安全偏好的重要机制。

---

〔54〕 研究者发现现实中这些不同领域内的厂商提供的隐私条款的确存在与其业务内容相关的差异。*See* Florencia Marotta-Wurgler, “Self-Regulation and Competition in Privacy Policies”, 45 J. Legal Stud. S13 (2016).

〔55〕 Daniel J. Solove & Woodrow Hartzog, “The FTC and the New Common Law of Privacy”, 114 Colum. L. Rev. 583 (2014).

〔56〕 Ariel Porat & Lior Jacob Strahilevitz, “Personalizing Default Rules and Disclosure with Big Data”, 112 Mich. L. Rev. 1417, 1468－1469 (2014).

〔57〕 Ben-Shahar, *supra* note〔10〕, at 24.

〔58〕 Troyen A. Brennan, “Causal Chains and Statistical Links: The Role of Scientific Uncertainty in Hazardous-Substance Litigation”, 73 Cornell L. Rev. 469, 491－493 (1988).

就大规模个人信息泄露事件所导致的风险而言，企业如果因侵犯个人权利而被要求承担民事赔偿或行政罚金责任，那么以此为基础，企业还应被要求强制购买责任保险。这种强制责任险能够更有效地保证用户在相关风险日后落实为实际损害时，可以就实际损害获得完美填补。但更重要的是，借助强制责任保险制度，保险公司将在数据隐私和信息安全领域全流程介入，而这除了使得有关个人信息权的权利制度和民事救济制度变得更有可能落在实处，还有望带来更好的风险信息收集、风险定价和系统性风险管理。

当然，除了企业责任险之外，市场上已经较为常见的，还有个人信息安全类保险。这类保险无疑对于降低个人风险、填补损失有重要价值。但与其他许多领域类似，当可以为预期损害购买保险时，个体自身进行合理数据隐私防范的激励也可能会降低，即出现道德风险问题。而在数据隐私语境中，由于每个个体随意披露本人数据的行为有可能增加他人数据隐私风险，因此保险外部性(insurance externality)是信息安全保险市场缺乏效率的一个可能来源。〔59〕个人信息安全险的这一问题，反过来更说明推动、建立强制企业责任险的必要性。

3. 数据权属与数据定价

企业竞争维度上的机制设计相对更复杂，需要同时照顾到先发企业投资于收集、处理个人信息并基于此生产高价值数据资源的激励，以及后发企业充分利用现有资源寻求创新、避免形成垄断等市场竞争价值。

如前所述，无论是在个人还是企业的层面，目前有关数据权属安排的常见设计建议，总体上都依循着财产规则(property rule)的思路，即试图将由个人信息生出的数据资源进行分类之后，一部分的排他控制权交付个人，另一部分的排他控制权交付企业，而对于个人或企业各自控制的资源，第三方只有在获得前者自愿同意的前提下才能通过交易的方式获取或加以利用，包括直接抓取或间接获取等违背权利人控制原则的方式都不为法律所许可。

根据法律经济学的一般看法，财产规则的优势在于通过确保交易的自愿性来避免资源转移无效率，但其劣势则在于当交易成本较高时，有效率的交易可能难以发生。特别是在企业竞争维度，基于策略性考虑，为维护并巩固自身市场地位，拥有高质量数据资源的企业通常追求通过协议和技术在最大限度上控制其他企业对相同数据资源进行利用的对价和方式。而在现有的强调企业排他控制数据资源的模式之下，由于上述策略性利益思维促使企业追求数据独占，更有助于促进企业间数据交易和定价的机制，也一直未能获得充分发展。

如前所述，对于企业专有数据权妨碍数据资源有效流转和利用、助长垄断的问题，以欧盟倡导的数据可携权为代表的解决思路，是用个体控制权节制企业专有权，由此撬动日趋封闭的数据资源配置格局。在 GDPR 通过后不久，包括 Google、Facebook、Microsoft 和 Twitter 在内的几家巨头平台公司之间，率先宣布达成了实质上在一定范围内落实可携权的机制安排：这些企业之间在对现有 API 模式升级的基础上，通过建立一套允许用户在平台间直接传输个人数据的系统，实现用户在平台间的灵活迁移。〔60〕表面上看，这一安排反映了可携权的要求，对个体用户有利，也促

〔59〕 Ben-Shahar, *supra* note〔10〕, at 15－16.

〔60〕 该项目启动于 2017 年。*See* Data Transfer Project, https://datatransferproject.dev/, last visited 2018－12－02; Introducing Data Transfer Project: An Open Source Platform Prompting Universal Data Portability, Google Open Source Project, Jul. 20, 2018, https://opensource.googleblog.com/2018/07/introducing-data-transfer-project.html, last visited 2018－12－02. 谷歌明确指出这一项目是为 GDPR 合规之目的而开发。William Malcolm, Our Preparations for Europe's New Data Protection Law, May 11, 2018, https://www.blog.google/outreach-initiatives/public-policy/our-preparations-europes-new-data-protection-law/, last visited 2018－12－02.

进了可共同利用的数据资源池的扩大。但对于大多数用户而言，当能够在大平台之间“自由”迁移时，他们将自身的服务需求——以及其数据——迁移到这些大平台之外的其他企业的可能性，或许也会进一步降低，而市场本身的集中度甚至可能因此提高。

相比而言，另一个更为激进的可能思路是基于“责任规则”(liability rule)，重新设置企业数据权益的机制。这一思路受到波斯纳和韦尔(Weyl)极富创造力的机制设计构想启发。[61] 他们指出，任何“财产规则”(property rule)本质上都必然带来某种程度上的垄断效果，因此如果使资源在充分流转的基础上实现有效率配置，是社会所期待的目标，那么对于任何资源占有者而言，其受到的保护都应采取责任规则而非财产规则的模式。在责任规则模式下，资源占有者对其资源不享有排他的控制权利，只要要求第三方支付客观厘定的对价，资源占有的转移就可发生，无论资源占有者本人是否同意[62]——因此，责任规则有时也被称为“强制交易规则”。

责任规则的可能问题当然在于，当资源转移并非基于自愿交易发生时，如果没有其他机制保证交易价格合理，那么资源的强制转移也可能导致无效率的配置结果，并破坏有效的投资激励。但波斯纳和韦尔的贡献在于，他们指出责任规则的上述缺陷完全可以通过资源占有人“强制报价加第三方征税”(Harberger tax)的方式获得有效处理。具体而言，对于任何一类资源而言，理论上，借助不断发展的数据信息科技，法律都可以要求当前占有者对其占有的资源进行登记，并且自行给出主观估价，而任何第三方只要愿意支付这一估价，相关资源的权属就要转移给该第三方。同时，对于占有者当前占有的资源，政府会根据占有者自身提出的估价征税，而对税收比例的妥善设计，可以有效抑制占有者对其所占有的资源给予过高估价的激励。[63]

尽管波斯纳和韦尔在讨论时并未直接以数据资源为对象，但这一基于责任规则设计促进资源流转的机制的思路，对于未来有关企业数据权益的制度安排有重要启发。数据资源的估值本身的确有一定难度，而数据价值至今甚至无法反映在企业的资产负债表之中。但在资本市场上，投资人对于数据企业所拥有的数据资产的价值，已经在逐渐形成一些基本的分析和估测思路。[64] 如果基于责任规则的强制报价能够得到确立，这反而也应有助于进一步推动数据资源定价机制的形成。强制交易规则的落实，相比于价格不透明、交易受控于资源控制方的市场状态，更有利于降低新兴企业获取数据、参与竞争的门槛。进一步来说，对于那些确实高度关注数据排他独占利益的企业来说，如果为了确保独占，其甘愿在给出极高报价的同时支付足额税收，那么这也有利于保证独占权人为其独占权益向社会支付相应的对价。尽管对于习惯了传统财产权观念的法律人来说，上述责任规则的思路无疑会有不小冲击力，但既然承认数据资源不同于传统资源，那么至少在数据资源权益安排上接受创新，或许也并非过于激进。

4. 数据劳务市场机制设计

如果“数据作为劳动”(DaL)被视为人工智能持续发展前景下更为可欲的生产关系形态，那么

---

〔61〕 *See generally* Eric A. Posner & E. Glen Weyl, “Property Is Only Another Name for Monopoly”, 9 J. Legal Analysis 51 (2017). 财产规则和责任规则的概念来自法律经济学早期的经典理论框架。*See* Guido Calabresi & A. Douglas Melamed, “Property Rules, Liability Rules, and Inalienability: One View of the Cathedral”, 85 Harv. L. Rev. 1089, 1089 (1972).

〔62〕 Posner & Weyl, *supra* note〔61〕, at 58 - 59.

〔63〕 *Ibid.*, at 66 - 84.

〔64〕 例如，Lisa Morgan, “How Valuable Is Your Company's Data?” InformationWeek, Mar. 14, 2018, https://www.informationweek.com/big-data/big-data-analytics/how-valuable-is-your-companys-data/a/d-id/1331246, last visited 2018 - 12 - 02.

为促使从当前占据主导地位的“数据作为资本”（DaC）向“数据作为劳动”的范式转进能够实际发生，仅靠赋予个体对其自身个人信息的某种控制权，显然是不够的。特别是在人们早已习惯了免费互联网模式下以数据换服务的宏观社会契约这一前提下，路径依赖会强化个体基于理性或非理性的理由，选择放弃这种控制权，并由此不再享有持续参与数据资源价值积累与分配的权利。〔65〕

但即便要另起炉灶，将个体产生数据的各类行为理解为“劳动”本身，而不只是数据资本进行加工的客体，这种理念也必须要在对此类数据劳动可以实现合理定价的基础上，才有可能获得落实。那么，对数据劳务进行定价的机制是否可能，又应如何设计？

尽管当前免费服务换免费数据的主导商业模式限制了人们对此类定价机制的想象，但在实践中，对数据劳务进行定价显然从来都不是天方夜谭。研究者对用户个人信息商业价值的一些粗略估算当然可以提供初步的线索。〔66〕但更直接的观察是，人工智能行业事实上一直以来都在大规模使用人工进行数据标识和分析，并对这些人工劳务支付报酬。〔67〕而包括 Amazon、Apple 和 Microsoft 等在内的以生产力为导向的互联网企业（相对于 Facebook 和 Google 等采用媒体化商业模式的企业），为了获得更多、更高质量的生产型数据，也都曾经或正在寻求将机器学习获利的至少部分价值，分享给为其提供相关数据的个体用户。一个鲜明的例子就是，作为搜索引擎市场中的后发参与者，为了弥补其与 Google 相比因数据积累不足而在算法训练资源方面存在的劣势，Microsoft 在开发 Bing 搜索时，直接对用户就其使用 Bing 搜索的行为提供现金报酬。〔68〕

企业层面的自发安排，在逻辑上并不难理解，并且完全可以作为探索未来数据劳务定价机制的起点。而未来尤其亟待探索的，是如何更为广泛地使劳动者在生产活动的原始语境中制造的劳务数据能够获得定价以及相应劳务支付。只有这样的定价机制能够实现，例如在训练语言翻译的智能算法时，机器学习才可能更广泛地以高水平人类翻译家的翻译行为直接形成的高质量数据为学习对象，而不是像现在这样主要依靠标记员对免费网络信息标记形成的数据——或至多再加上互联网公司招募的廉价校对员为机器翻译的成果提供反馈而形成的数据。

但需要指出的是，依靠生产力导向的技术企业——特别是人工智能企业——自发的探索和实践，显然还无法确保体现“数据作为劳动”理念的生产关系安排能够在宏观层面完整形成。如前文提到，在当前买方垄断的数据市场条件下，有理由认为，即使是已经选择为获取数据付费的企业，其付费的数据范围和信息主体对象范围，也是相对有限的，其就数据劳务支付的对价在算法生产剩余中所占的比重则较低。〔69〕而且，有理由怀疑，从长期趋势上看，类似付费安排的范围可能会变小、对价可能会变低，而不是相反——因为尽管机器学习和深度学习在一个阶段之内仍会对人类生产、标注的数据高度依赖，但人工智能的发展完全可能最终超越这个数据依赖阶段，而这意味

---

〔65〕 Arietta-Ibarra et al., *supra* note〔44〕, at 3－4.

〔66〕 “How Much Is Your Data Worth? At Least $240 per Year. Likely Much More.”, Wibson, Jan.8, 2018, https://medium.com/wibson/how-much-is-your-data-worth-at-least-240-per-year-likely-much-more-984e250c2ffa, last visited 2018－12－02.

〔67〕 参见甲子光年：《“数据折叠”：今天，那些人工智能背后“标数据的人”正在回家》，36 氪，https://36kr.com/p/5119805.html，最后访问时间 2018－12－02。

〔68〕 Tom Warren, “Microsoft is Now Paying People to Use Bing in the UK with its Rewards Scheme”, The Verge, Jun.1, 2017, https://www.theverge.com/2017/6/1/15723566/microsoft-rewards-uk-features, last visited 2018－12－02.

〔69〕 Aindrajit Dube, Jeff Jacobs, Suresh Naidu & Siddharth Suri, Monopsony in Online Labor Markets, 2018, https://irs.princeton.edu/sites/irs/files/monopsony_crowdsourcing_resubmission_sept_25_2018.pdf, last visited 2018－12－02.

着人工智能企业自主设计数据劳务报酬安排的动力会变得可能更低。如果长期趋势的确如此，在现阶段借助类似集体谈判等机制，〔70〕尽可能提高数据劳动者与使用生产力数据的企业之间约定数据劳务关系时的谈判地位和筹码，就可能具有更高的紧迫性。

## 五、结　　语

法学研究和讨论的议题滞后于实践发展本属常情。但在数据隐私问题上，由于相关实践变动过于迅速，研究者知识、思路和视野的更新与扩展就更容易显出滞后。借助理论梳理和分析，本文提示，在试图回应当代数据隐私挑战时，法学界截至目前为自身设定的权利建构议题局限性极大。在个体权益维度上，仅靠赋予个人信息主体以控制权，无法保证妥善平衡个体偏好和社会总体福利的数据隐私安排，能够最终通过自愿授权和自由选择达成。在企业竞争维度上，仅凭个体赋权未必能有效冲击、重构资源集中化、市场垄断化的格局，且数据隐私保护话题还可能被先发企业裹挟，成为其推进自身资源控制诉求的筹码。在生产关系维度上，尽管个体控制是数据劳动者主体地位得到承认的先决条件之一，但若没有行之有效的劳务市场安排及定价机制，信息主体仍只会继续在自由选择、自由交易的基础上辅助数据资本的积累。

由此看来，在当下和未来，法学界对数据隐私问题的思考和讨论，应尽快从有关个体权利建构的形式化议题，转入富有想象力的机制设计探索。机制设计当然不是法学界凭借一己之力能够完成的——甚至可能主要不会由法律人完成——，但围绕相关机制设计可能产生的法律问题，将是法学研究能够真正有意义地为社会做出实质——而非假想式——制度贡献的领域。

**Abstract** "Data privacy problems" encompass a wide range of political, economic, legal and ethical problems resulting from public agencies and commercial entities' processing of personal data. Legal scholars have long focused their deliberation on the formalistic question of how to formulate and enshrine a right to personal information through legislation. In reality, however, rapid developments in market practices and technologies have already moved the data privacy problems beyond such formalistic concerns and witnessed complex problems unfolded in the dimensions of individual interests, market competition, and relations of production. Against such general backdrop, legal scholars must pay more attention to mechanism design questions in relation to regulating data-related contractual arrangements, managing data risks, enabling data exchange and trading, and pricing data labor. That way legal studies may meaningfully contribute to the human society's overall response to the data privacy challenges.

**Keywords** Data Privacy Problems, Personal Information, Competition, Mechanism Design

（责任编辑：黄韬）

〔70〕 Arrieta-Ibarra et al., *supra* note〔44〕.