个人数据治理的体制变革：从个人决定到社会许可

高富平*

摘要 伴随数字技术迭代发展和深度应用，数据与人工智能正驱动着社会不断变革，如何在充分保障各方权益的前提下，释放数据要素价值，已成为各国个人数据治理制度面临的核心难题。数据资源化(要素化)利用要求数据实现社会化重用，即数据具备可获取性且使用者享有使用方式的决定权。然而，以个人决定为基础的现行个人数据治理制度，与数据资源化利用的现实需求之间存在结构性张力。为此，各国正积极探索适应时代需要的制度变革路径。其中，美国持续完善“负责任数据治理”体制，欧洲则通过修法扩张“合法利益”的适用范围并适度放松合规监管，以回应个人数据资源化带来的制度挑战。在制度重构探索中，社会契约理论被引入个人数据治理领域，为重新审视个人与社会在个人数据治理中的权利配置与制度安排提供了新的理论视角。具体而言，应当以社会许可机制为基础重构合法性基础体系，并对信息主体与处理者之间的权利义务关系作出相应调整。这一转向将有助于个人信息保护法摆脱“权利法”的路径依赖，实现向“行为法”的彻底转型，从而破解个人保护与资源利用的制度冲突，实现信息主体权益保护与促进数据社会化重用的双重目标。

关键词 个人数据 个人数据治理 个人决定 社会契约理论 社会许可

一、引　　言

以人工智能为核心驱动力的智能经济正在成为经济发展的新引擎。[1] 2025 年国务院印发《关于深入实施“人工智能＋”行动的意见》，明确了实施“人工智能＋”行动的总体要求、发展目标和重点方向，加快智能经济和智能社会发展。人工智能作为高度依赖数据的计算机技术，对数据

* 华东政法大学法律学院教授、法学博士。

〔1〕 参见彭绪庶：《“人工智能＋”的战略意义与推进路径》，载《经济日报》2025 年 9 月 23 日，第 10 版。

的可获取性和可利用性起着重要作用。我国与世界各国大体同期部署大数据战略，[2]并率先提出数据作为第五大生产要素的理念，[3]积极构建以促进数据流通利用为核心的基础制度[4]。其核心目的是促进数据的社会化重用，适配数字经济时代下日益增长的数据智能和数据分析的社会需求。

个人数据（又称个人信息，本文等同使用）是数据资源（我国称数据要素）中的重要组成部分。作为社会资源，我们需要从数据使用[5]入手探索其价值形成和实现（即要素化利用）的路径和方法，并据此构建制度规则。关于数据价值，学界普遍认为，碎片化数据难以彰显其应用价值，只有在与其他数据持续汇集、整理和集成的过程中才能释放价值，为 AI 模型训练和智能决策提供支撑。[6] 当数据关联个人，或者数据使用结果与个人紧密相连时（统称为个人数据或个人信息数据），数据资源化（要素化）利用面临个人保护与社会使用之间的紧张关系，即个人决定还是使用者决定的制度选择问题。由于大数据源于社会活动，数据及其使用难免与个人勾连或产生影响，如何平衡个人保护与数据社会使用（重用）成为数据要素化利用的关键。放眼世界，个人数据治理面临的制度困境本质是 20 世纪 70 年代建立的制度难以应对 21 世纪的新课题。

个人数据保护存在一个基本制度假设：个人数据是社会可利用的资源，[7]个人数据保护法旨在促进个人数据在社会流通利用。对这一制度逻辑的准确理解，有赖于对个人信息自决权的正本清源。德国法和德国学说中的个人信息自决权并非指个人控制其个人信息。[8] 个人信息自决是人权层面的一项原则，是个人自主、自由、自决等在个人信息处理中的体现，而非个人数据作为资源使用的一项制度。[9] 即使在人权层面，个人决定也不是欧洲个人数据保护立法的指导思想。从《关于个人数据自动化处理的个人保护公约》[10]至落实该公约的欧盟立法均采“合法性基础＋处理行为规范”的模式，而且处理行为合法与否需要在具体场景中加以判断，即数据主体权利是否得到尊重、数据控制者（对应我国“处理者”，本文统称为“使用者”）是否履行规定义务并以数据处理基本原则为兜底判断。欧盟《统一数据保护条例》（以下简称“GDPR”）肩负着保护个人与实现个

---

〔2〕 2015 年 8 月，国务院发布《促进大数据发展行动纲要》（国发〔2015〕50 号）。

〔3〕 2020 年 3 月，中共中央、国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》。

〔4〕 2022 年 12 月，中共中央、国务院公布《构建数据基础制度更好发挥数据要素作用的意见》，从数据产权、流通交易、收益分配和安全治理四方面初步搭建我国数据基础制度体系，提出 20 条政策举措。

〔5〕 《个人信息保护法》的基本术语是处理，而不是使用。这两个术语存在细微的差别，个人信息处理是从对主体权益影响的角度的规范，涵盖任何使用计算机（数字技术）对个人信息的操作行为；个人信息使用则是从使用者实现数据价值的角度，对信息或数据的操作行为。数据使用一定涉及处理行为，但处理行为涵盖范围要广于使用。本文以数据使用替代数据处理并不影响《个人信息保护法》的适用。关于数据使用的进一步研究，参见高富平：《数据使用理论——基于社会价值的数据重用秩序》，载《贵州社会科学》2025 年第 3 期。

〔6〕 参见毛俊响、王心怡：《我国数据治理法治化：挑战、定位与逻辑》，载《法律适用》2023 年第 12 期。

〔7〕 参见高富平：《基于规范目的的个人信息治理规则》，载《中国应用法学》2022 年第 6 期。

〔8〕 参见杨芳：《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》，载《比较法研究》2015 年第 6 期。

〔9〕 事实上，人们多忽略人权层面的决定权和资源使用的决定权的差异，而直接将个人决定延伸至资源使用决定。

〔10〕 该公约通过于 1981 年，并进行了多次修订。See Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108, 28 January 1981, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108; Council of Europe, Protocol amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, CETS No. 223, 10 October 2018, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=223.

人数据自由流通的双重目的。[11] 然而,这些立法愿景虽然美好且逻辑自洽,但是其制度设计背离初衷,不能实现个人数据流通利用的目的。[12] GDPR实施后的社会经济影响评估印证了笔者的判断。[13]

我国自2012年引入域外个人信息保护制度,[14]并于2021年制定《个人信息保护法》(以下简称《个保法》[15])。虽然有10年的探索,但是《个保法》仍然是"简化版"GDPR,在立法目的和立法模式上遵循了欧洲传统。《个保法》第1条兼顾个人保护和社会利用的双重目标,采取行为规范模式,构建了"个人信息处理合法基础+个人信息处理行为合法性"的规范框架。但从《个保法》的内容和实施来看,立法只对个人提供保护,忽略了对使用者利益、社会利益和公共利益的保护,同时亦设有个人对个人信息自主控制的特别规则。比如,合法性基础缺失了"处理者合法利益",限缩了社会主体合法获取和使用个人信息的空间;通过同意、重新同意和单独同意强化个人对个人信息使用过程的控制或决定。[16]《个保法》主要规范个人信息处理者(使用者)与个人之间的直接使用关系,而不允许个人信息处理者(在要素市场中称为数据持有者)对外自主提供,亦未为第三方提供从处理者间接取得数据的合法通道。[17] 故《个保法》既未给个人信息使用者以对外提供(流通)个人信息数据的权利,也未给潜在需求者(使用者)提供间接获得个人信息的渠道。由此,个人在法律

---

[11] GDPR的全称为《欧洲议会和欧盟理事会2016年4月27日关于个人数据处理中自然人保护、个人数据自由流通以及废除95/46/EC号指令的(EU) 2016/679号条例》[REGULATION (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data And on the Free Movement of Such Data, And Repealing Directive 95/46/Ec (General Data Protection Regulation)]。

[12] 参见高富平:《GDPR的制度缺陷及其对我国〈个人信息保护法〉实施的警示》,载《法治研究》2022年第3期。

[13] See John M. Yun, *A Report Card on the Impact of Europe's Privacy Regulation (GDPR) on Digital Markets*, 31 George Mason Law Review Forum 104 (2024).(虽然GDPR适度增强了用户数据保护,但也引发了不利影响,包括初创企业活动减少、创新减少以及市场集中度增加。此外隐私保护的收益被合规成本所抵消,而合规成本对小型企业的影响尤为严重。)Knut Blind, Crispin Niebel & Christian Rammer, *The Impact of the EU General Data Protection Regulation on Product Innovation*, 31(3) Industry and Innovation 311, 311-335 (2024).(以德国企业为样本的实证研究表明,GDPR导致受此新数据保护条例影响的企业创新活动发生转变,从而使得渐进式创新增加,而根本性创新减少。由于AI需要大量数据集,通常涉及个人数据,GDPR的引入可能会使这些数据的使用和分析变得复杂,从而延迟,甚至阻碍某些激进创新的发展。)Francesco Decarolis & Cristiana Firullo, *Unlocking Growth: Exploring the Economic Impact of GDPR for Tomorrow's Europe*, CliffordChance, 4 November 2025, https://cliffordchance.eventogy.com/c/gdpreconomicimpact/registration.(GDPR带来了巨大且不均衡的经济成本。固定和运营合规支出数额巨大且具有重复性,尤其是与法律解释、文件记录和持续监控相关的支出。间接影响包括数据获取成本增加、跨境数据流动减少,以及数据驱动行业风险投资和创新强度的明显放缓。同时指出,程序权利的增强提高了透明度,但对个人保护效果是有限的,仅部分转化为福利收益,因为有限理性、用户体验恶化、同意疲劳和偏好差异限制了个人有效行使控制权的能力。)

[14] 2012年12月28日,第十一届全国人民代表大会常务委员会第三十次会议通过《全国人民代表大会常务委员会关于加强网络信息保护的决定》。

[15] 为了避免我国《个人信息保护法》与域外"个人数据保护法"的切换问题,本文以"个保法"泛称个人信息/个人数据保护法,而以《个保法》指代我国的《个人信息保护法》。

[16] 依据《个人信息保护法》,个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息(第22条),个人信息处理者向其他个人信息处理者提供其处理的个人信息(第23条),个人信息处理者向中华人民共和国境外提供个人信息(第39条)抑或个人信息公开(第25条),都需要通过重新同意、单独同意或者再次告知等形式与个人重新建立使用关系。

[17] 同前注[7],高富平文。

形式上成为个人数据要素化利用的决定者，以及数据要素市场的主导者。

显然，《个保法》省去了“合法利益”和相关例外条款，[18]强化了个人同意并将其贯彻到一切个人信息数据利用的环节。在全力推进数据要素市场建设、发展人工智能＋战略和促进整个社会数智化转型的今天，我们需要认真思考《个保法》及围绕其建立的相关法律规则面临的挑战及改革问题。对于个保法缺陷、制度失灵、实施困境等问题，学术界已经在既有法律框架下作了深入的探讨，并提出诸多修补意见。[19] 笔者也对 GDPR 所代表的个人数据保护制度的根本缺陷作出深刻分析，并对产生于域外特殊时代和社会背景下的个人数据保护制度，是否还能够用前网络时代的法律原则解决万物互联泛在网络（网络化、数字化、智能化）时代的问题，作出深入研判，[20]同时还提出我国个人信息保护亟须范式转型：从单一保护个人权利转向保护相关者利益的数据治理范式。[21] 本文试图在此基础上继续挑战个人信息保护制度的根基，即同意制度，寻求适合当下的保护个人权利及实现个人数据重用的制度范式。为此，本文主张摒弃个人同意制度，转而迈向社会许可模式，在保障个人权利的前提下，推动数据社会化使用的最大化，实现数据要素的社会价值。

二、个人数据治理的权利错配与制度困境

个人数据保护法以保护数据主体权利为目标，对于个人数据社会利用的制度假设是：只要遵守个人数据保护法保护个人权利，那么个人数据就可以自由流动利用。但当下数据要素化利用需要控制和秩序，亟须建立一种能够支持大规模汇聚和集成数据并从中提取模式（或训练模型），再运用智能模型处理分析数据，支撑社会运营和各种决策的数据使用秩序。数据要素化利用与个人数据保护制度设计的初衷相悖，二者在现实层面已形成明显张力与冲突。[22]

（一）同意机制的失灵与权利错配

个人数据保护法旨在保护个人自主权（主体权利）不因个人信息处理行为而受到侵害，其保护逻辑可概括为：个人数据是关于个人的，个人是主体，因而个人（称为数据主体）为维护自己尊严、自由和隐私决定或干预数据的处理。虽然在立法上，个人数据保护法并未建立非经同意即不得使用的财产规则，但域内外均存在直接将数据主体自主权延伸至数据资源利用秩序的现象。

自个人数据保护制度创立至今，鲜有人承认个人享有个人数据使用决定权（实现数据要素价值），但是在实践中这种状态却导致了个人自主权（或自决权）被延伸至资源化利用的决定。其原因主要有两方面：一是在理论上，“个人数据受保护”被理解为人权，这使得个人在数据处理中的权利保护被绝对化，使其个人权利优先于代表社会利益的合法数据使用者。[23] 二是个保法实施的

---

〔18〕 相对而言，欧盟 GDPR 除了承认可援用“合法利益”作为商业使用的法律基础外，还有大量例外条款来保护公益目的和特殊利益。例如，GDPR 第九章第 85 至 91 条。

〔19〕 参见丁晓东：《人工智能背景下个人信息保护制度的挑战与应对》，载《政治与法律》2026 年第 1 期；付新华：《生成式人工智能对个人信息保护法的结构性冲击及应对》，载《法学论坛》2025 年第 6 期；叶雄彪：《生成式人工智能背景下的个人信息保护：范式转换与规则完善》，载《法学家》2025 年第 4 期。

〔20〕 同前注〔12〕，高富平文。

〔21〕 参见高富平、尹腊梅：《数据上个人信息权益：从保护到治理的范式转变》，载《浙江社会科学》2022 年第 1 期。

〔22〕 参见巩姗姗：《数据财产权与个人信息权益的冲突与调适》，载《中外法学》2025 年第 6 期。

〔23〕 尽管立法者认为需要平衡个人利益和社会利益、公共利益，但在法律设计中仍然给了数据主体权利以优先保护。GDPR 第 6 条虽然将“数据控制者或第三人的合法利益”作为数据处理的合法性基础，但是这种合法利益需要与数据主体利益相平衡，冲突时优先保护主体权利。

结果。实践者逐渐发现,同意是最好用的合规手段。无论是否存在法定事由,只要有机会与个人(用户)交互,那么组织一定会索要“同意”,以作为证明合规的最佳手段和兜底保障。由于同意清单冗长、内容泛化,与法律文本中的同意大相径庭,根本达不到对个人保护的法律效果,反而营造出个人数据的使用是由个人授权(决定)的假象,促成了个人决定数据使用的“事实”。

我国《个保法》创造性地设计了“同意”“重新同意”和“单独同意”,将个人同意贯彻到个人信息处理的各个环节,不允许处理者自主提供。[24] 虽然《个保法》第23条规定处理者可以对外提供,但是须“取得个人的单独同意”。单独同意阻碍了数据社会化重用,若严格执行将制约个人数据的流通与利用。

在数字社会,个人数据并不完全涉及个人利益,也包括使用者利益。[25] 个人数据具有社会资源属性,[26]而不属于个人资源,个人并没有单一的决定权。个保法制度设计的初衷是保护自然人主体地位,保护尊严、自由和隐私。当保护自然人主体权利的制度直接延伸到资源使用秩序时,就将出现制度错配问题,导致数据资源利用秩序走不出个人控制的“阴霾”。

问题不仅在于以同意为核心的个人决定权错配于数据资源利用秩序,还在于同意制度本身是否切实地保护了个人权利。现有知情同意机制建立在理性个体的经典模型基础上,即一个理性个体可以阅读和理解隐私政策,权衡获取服务与被收集信息之间的利益冲突,并作出明智的选择。[27] 但这一假设难以成立。早在2010年,经济合作与发展组织(OECD)即开始对其30年前发布的个人信息保护原则进行反思。[28] 之后,微软公司策划和组织四场对话和一次世界隐私峰会,讨论OECD原则更新问题,并于2013年形成一份总结报告。[29] 总体上,与会者认为,在大数据时代个人控制可能会给数据处理者和数据主体带来重大负担。大数据不仅很大,且收集和处理的频率较高,以至于大多数人都无法接受授权同意的频率,严重依赖个人通知和同意的隐私框架既不可持续,也不可取。2023年,纽约大学的韦尔胡尔斯特(Stefaan G. Verhulst)教授对于知情同意的缺陷作了系统总结。他认为,实践中同意沦为用户协议“点击同意”的一揽子操作,存在许多缺点:(1)要么加入,要么退出的二元选择;(2)形式化同意无法实现真正的知情同意;(3)多个主体的个人同意难以代表集体;(4)同意范围有限。[30]

个人同意不仅流于形式,而且还存在越权甚或侵权风险。提供关于同种族、同性别和同年龄段人群的信息可能会造成对多人的政治、经济歧视或剥削。另外,数据是非竞争性的、非排他性的、不可耗尽的,具有公共物品性质,赋予数据主体决定权意味着个人数据“私有化”,引发数据市场化和商品化的严重担忧。[31] 在资源化利用背景下审视同意,应遵循同意的制度宗旨,重新设计

---

〔24〕 参见《个人信息保护法》第22条。

〔25〕 参见高富平:《个人信息使用的合法性基础——数据上利益分析视角》,载《比较法研究》2019年第2期。

〔26〕 同前注〔21〕,高富平、尹腊梅文。

〔27〕 See Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harvard Law Review 1880,1883 (2013).

〔28〕 See Michael Kirby, *The History, Achievement and Future of the 1980 OECD Guidelines on Privacy*, 1 International Data Privacy Law 6, 6-14 (2011).

〔29〕 See Fred H. Cate & Viktor Mayer-Schönberger, *Notice and Consent in a World of Big Data*, 3 International Data Privacy Law 67, 67-73 (2013).

〔30〕 See Stefaan G. Verhulst, *Operationalizing Digital Self-Determination*, 5 Data & Policy e14 (2023).

〔31〕 See Jonathan Montgomery, *Data Sharing and the Idea of Ownership*, 23 The New Bioethics 81, 81-86 (2017).

实现“知情同意”目标的机制，寻找替代个人同意更有效的方案。

（二）数据资源化利用的制度障碍

人工智能技术本质上是数据驱动的计算技术，数据既是机器学习的原材料，同时又是智能模式分析处理的对象。数据具有资源价值，我国将之表达为数据是生产要素。无论模型训练或机器学习，还是智能系统应用下的数据分析（知识输出）都需要汇聚和集成大规模数据。

AI 研究组织 Epoch2024 年的一项研究声称，按照目前的速度，人类生成的互联网数据总量最早可能在 2026 年耗尽。[32] 虽然合成数据可以缓解某些数据获取问题，但也无法完全捕捉到真实世界数据的细微差别，影响 AI 模型的准确性和可靠性。因此，AI 研发和应用终究还是需要解决数据可获用性（data availability）[33]问题。

数据可获用性涉及两个层面：一是初始生成的未加工整理的数据（原始数据）的获用性；二是合法采集和获取后经加工整理的数据集（整理数据）的获用性。其一，当数据关联个人或可能用于个人时，个人对数据的控制或维权力量增强；其二，原始数据生成者（持有者）对数据保护意识和能力增强，待价而沽。[34] 我国在全球率先提出数据作为生产要素的理念，目的在于借助市场力量化解经加工整理的数据集的供需矛盾。但并未考虑第一个层面的数据可获用性问题。一旦这些数据涉及个人或分析使用指向个人，就存在“谁享有决定权”的问题。

数据可重用是数据区别于其他资源最主要的特征。从主体的角度，数据重用既可以为原持有者使用，亦可以提供他人使用，在我国称为数据流通。从目的的角度，数据重用既包括在初始目的范围内不断重复使用（复用），也包括用于其初始收集目的之外的其他目的，即“更新目的重用”（repurposing）[35]。为实现数据资源价值，必须支持数据在更新目的和更新主体情形下的社会化重用，即数据可以在不同主体之间变换目的的流通利用。这便是本文主张的数据重用内涵。

各种组织一般按照数据生命周期管理数据使用。这意味着在数据初始收集目的实现时，原始数据即应当删除。这样的合规管理可以容忍原使用者在原目的范围内复用，但是不能承载更新主体和目的的数据重用。数据重用的现实需求与个保法的目的特定原则之间横亘着显著张力，制约了数据的可获用性和可重用性。因此，我们需要检讨国际社会在 20 世纪 80 年代形成的数据保护原则的正当性、合时宜性。

三、个人数据治理的域外制度探索与变革

个保法的理念和制度建立在前网络和数据智能时代，当时只关注个人数据处理行为对个人的影响和危害，而今天我们还关注个人数据如何合法和安全地使用以创造社会价值。在应对这一时代命题上，美国一直基于“正当信息准则”规制路径，使个人保护与社会使用之间的平衡保持一定弹性，而欧洲（本文限于欧盟和英国）因采取以个人权利为核心的制定法体制，不得不通过修法和

---

〔32〕 See Pablo Villalobos et al., *Will We Run Out of Data? Limits of LLM Scaling Based on Human-Generated Data*, arXiv:2211.04325 (2024), https://arxiv.org/abs/2211.04325, visited on 15 May 2026.

〔33〕 英文 availability 本义是可使用，但先要获取才能使用，因此，“获用性”能够准确表达数据可以获取和使用两重含义。

〔34〕 参见孙笑侠：《论数字权利的关系变异》，载《法律科学》2025 年第 6 期。

〔35〕 Shawn Ogunseye & Jeffrey Parsons, *Responsible Data Repurposing: A Conceptual Foundation*, proceedings of the 58th Hawaii International Conference on System Sciences 2025.

调整法律实施的方式不断修正法律规则。

（一）合法利益的重塑：欧洲的体系纠偏

“合法利益”是欧盟1995年《个人数据保护指令》和2016年GDPR个人数据处理的重要合法性基础，作为与数据主体基本权利和自由相平衡的数据使用的正当理由。2014年第29条工作组对合法利益作了较为狭窄的解读，[36]而且使用数据的合法利益需要与数据主体的基本权利和自由相平衡，在冲突时应当优先保护数据主体权利，极度限缩了可适用的范围。

欧盟数据保护委员会（EDPB）于2024年发布第28/2024号意见，[37]认可合法利益可作为AI模型开发与部署的合法性基础，但须逐案通过测试判断，若确属匿名模型则GDPR不再适用。次年，法国国家信息与自由委员会（CNIL）发布以合法利益为法律依据的《指南和建议》[38]，明确指出在符合某些特定条件时，基于公共内容获取的个人数据用于人工智能模型训练可依据GDPR的合法利益原则认定为合法。德国则在Meta案中，以法院判例的方式宣布，Meta使用个人数据用于人工智能训练具有“合法利益”，实质上也承认合法利益可以作为人工智能训练的合法性基础。[39]

自2012年启动GDPR起草以来，欧盟一直努力在公民基本权利保护理念下构建数据保护和数字经济立法体系，但是如今却发现这些立法不仅没有给欧盟数字经济发展带来有利环境，反而使欧洲在人工智能研发和应用方面与美国差距拉大。欧盟委员会于2025年11月19日发布数字综合监管条例提案，[40]旨在简化、优化和调整现有的数字规则，核心目标是加强协调，实现清晰度更高、成本更低和更连贯的立法框架。该提案同时对GDPR作出修订。该修正案草案于2025年11月初首次公开，[41]远远超出了改革GDPR的最初提议，被认为用隐私来满足人工智能热潮。

---

〔36〕 仅仅将合法利益判断因素归结为以下方面：(a) 个人（雇员、消费者、病人）和数据控制人（雇主、居于优势地位的公司、健康服务提供者）之间的地位；(b) 数据处理的环境或场景（数据处理者与数据控制人之间的合同关系）；(c) 该个人的合法预期。See Article 29 Working Party ，Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC，WP217，9 April 2014，https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

〔37〕 In its Opinion on AI Models the EDPB addressed the following topics：(i) when and how AI models can be considered anonymous；(ii) whether and how legitimate interest can be used as a legal basis for developing or using AI models；and (iii) what happens if an AI model is developed using personal data that was processed unlawfully.See European Data Protection Board，Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models，Adopted on 17 December 2024.

〔38〕 法国国家信息与自由委员会（CNIL）于2025年6月17日发布法语指引，对GDPR第6条(1)(f)合法利益适用于AI训练作出权威解释。参见法国国家信息与自由委员会网站，https://www.cnil.fr/en/decisions/lignes-directrices-recommandations-CNIL，2026年5月15日访问。

〔39〕 See Jenny Gesley，*Germany: Court Allows Meta to Use Data from Public Social Media Profiles to Train AI*，7 July 2025，https://www.loc.gov/item/global-legal-monitor/2025-07-07/germany-court-allows-meta-to-use-data-from-public-social-media-profiles-to-train-ai/.

〔40〕 Digital Omnibus Regulation Proposal，19 November 2025，https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal.

〔41〕 See Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679，(EU) 2016/1036，(EU) 2016/1037，(EU) 2017/1129，(EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures，https://storage.activemind.legal/wp-am-legal-cdn/wp-content/uploads/EU-Commission-GDPR-reform-2025-05-21.pdf.

脱欧后的英国不断探索和强化数据立法改革，于 2025 年通过了《数据使用与访问法》(DUAA)[42]。该法除了修订英国数据保护法外，还带来重大变革，包括(1) 将“科学研究”定义为任何可合理描述为科学的研究；(2) 引入“公认合法利益”作为处理个人数据法律依据；(3) 完善目的限制原则，细化个人数据原始处理与收集目的兼容的处理情形；(4) 打破没有人类参与的自动决策对个人数据使用的一些限制；(5) 控制者只需响应有明确数据主体的访问请求，对信息和个人数据进行合理和相称的搜索，维护数据主体的权利。依据 DUAA，“合法利益”可以作为 AI 训练使用数据的合法性依据。

综上，欧盟和英国现在已经接受“合法利益＋数据合规”作为 AI 模型训练的合法性基础，这为基于公开收集的个人数据进行人工智能模型训练提供了路径。这说明欧洲数据立法在反思和改革，只是因路径依赖而很难出现颠覆性的变革。

（二）负责任数据治理：美国的制度变革

美国在联邦层面没有制定统一的个人数据保护法，但有特别立法和普遍接受的“正当信息准则”，并在此前提下，通过普通法的救济体制发展出灵活保护规则。[43] 也正因此，美国个人数据保护制度一直处于发展变化之中。

早在 2006 年，凯特(Fred H. Cate)[44]即提出了所谓的“基于使用的体制”(use based system)，认为数据收集本身不应受限制，只有数据的使用才应当受到规制。其核心思想大致可以概括为开放收集、规范使用、损害救济。之后他与舒恩伯格(Viktor Mayer-Schönberger)共同领导微软隐私原则修订专家组，并在综述中概括了研讨会的共识：这些新方法必须将责任从数据主体转移到数据使用者，并将重点放在负责任的数据管理(responsible data stewardship)可追溯性上，而不仅仅是其合规性，同时确保隐私期待和保护要求得到实现。[45] 更加关注适当、负责任地使用，可能会实现更有价值的数据流和更有效的隐私保护之间更实用、更敏感地平衡。[46]

2014 年白宫大数据工作组的研究报告《大数据：抓住机会，发挥价值》[47]认为，长期坚持的“知情和同意”体制可能很快变得不合时宜，规制数据的使用可能成为大数据时代保护隐私的唯一方式。报告称之为“负责的使用框架”(a responsible use framework)。这一框架有两大好处：首先，它将责任从个人转移到收集、存储和使用数据的主体。其次，它也使数据的控制人和使用人对他们如何管理所掌握的数据及其引发的损害负责，而非仅明确他们在其收集时是否恰当地获得同意。[48]

---

[42] 《数据保护和数字信息法案》(Data Protection and Digital Information Bill，DPDI 法案)经过公众咨询和政府回应后，于 2022 年提交英国议会。两年后，DPDI 被替换为《数据使用与访问法》[Data (Use and Access) Act，简称 DUAA]，2025 年 6 月 19 日获得皇家御准批准，并分阶段生效。

[43] 参见高富平、王苑：《论个人数据保护制度的源流——域外立法的历史分析和启示》，载《河南社会科学》2019 年第 11 期。

[44] See Fred H. Cate, *The Failure of Fair Information Practice Principles*, in Jane K. Winn ed., Consumer Protection in the Age of the Information Economy, Ashgate, 2006, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972, visited on 28 December 2025.

[45] Cate & Mayer-Schönberger, supra note [29].

[46] Ibid.

[47] Executive Office of the President, *Big Data: Seizing Opportunities*, Preserving Values, May 2014, https://www.govinfo.gov/app/details/GOVPUB-PREX-PURL-gpo64868, visited on 15 May 2026.

[48] Ibid., p.56.

面对人工智能挑战，埃拉娜·泽德(Elana Zeide)教授[49]提出应重新定位隐私治理，从依赖个人控制和程序保障转向更具集体性、更积极和更预防性的方法，将隐私视为公共利益和集体责任。她提出了保护个人和集体隐私权的新范式，其关键要素为：(1) 从个人隐私概念转变为集体隐私概念；(2) 从被动治理转向主动治理；(3) 重新定位人工智能治理的目标和价值观。美国资深隐私法教授索罗夫与哈佐格敏锐地观察到，许多人工智能的训练都是基于未经同意、缺乏监督、没有限制或未考虑其可能造成的危害而大规模获取个人数据，而数据抓取几乎与所有核心隐私原则[50]相悖，使个人处于暴露和脆弱的境地。大规模的数据传输是基于一系列幕后处理而实施的，个人却无法参与其中，援用合法同意保护个人是不切实际的。爬取数据的真正影响只有在集体层面才能体现，而非个体层面，因而最重要的问题是数据收集、使用和转移是否符合公众利益。他们建议立法者应将系统化抓取、自动化地大规模收集和使用个人数据视为一种特权，服务于公共利益应作为获得抓取许可的前提。[51]

总之，美国学者基本上已经抛弃以个人权利为中心的数据保护模式，而在负责任治理框架下演绎负责任数据使用，强调集体隐私、社会整体利益和公共利益。也正是在这样的深度探索中，社会契约理论被引入个人数据使用规则的重塑之中。

四、个人数据治理的社会契约转向

随着数字技术深度应用，尤其是大数据、人工智能的兴起，人们逐渐认识到需要通过各种数据分享解决数据保护与数据流通的紧张关系，实现数据的社会价值。这迫使人们摆脱个人本位模式，重新思考数据权利的配置。《2021 年世界发展报告》[52]认为，打破当前数据治理的僵局需要一种新的数据社会契约。于是，在探索适合数字经济秩序的过程中，社会契约思想得到关注和应用。

(一) 社会契约兴起的理论基础

大致有三种理论支撑新社会契约理论，用以解决当前数据使用秩序和社会价值实现的问题。首先是数字公平理论。西班牙 IE 大学“变革治理中心”设立了“数字革命与新社会契约”研究项目，[53]提出数字经济(或数据经济)公平思想，认为“技术产生的机会、利益和权力的分配对社会中的每个人来说都是不平等的”[54]。公平的数据经济应当具备三个特征：一是公平的竞争环境将促

---

[49] See Elana Zeide, *Expanding the Paradigm: Generative Artificial Intelligence and U.S. Privacy Norms*, 1 Cambridge Forum on AI: Law and Governance e16, 1 - 10 (2025).

[50] 这些原则包括公平、个人权利和控制、透明度、同意、目的规范和二次使用限制、数据最小化、继续传输和数据安全。

[51] See Daniel J. Solove & Woodrow Hartzog, *The Great Scrape: The Clash Between Scraping and Privacy*, 113 California Law Review 1521, 1521 - 1584 (2025).

[52] See World Bank, *World Development Report 2021: Data for Better Lives*, 2021, https://www.worldbank.org/en/publication/wdr2021, visited on 15 May 2026.

[53] 项目自 2022 年设立，共分以下四部分：1. 数字经济；2. 数据经济；3. 数字时代的地缘政治；4. 新社会契约(正在进行，成果尚未发布)。See IE University Center for the Governance of Change, The Digital Revolution and the New Social Contract (Project led by Miguel Otero-Iglesias), https://www.ie.edu/cgc/research/new-social-contract-digital-age/, visited on 15 May 2026.

[54] See Miguel Otero-Iglesias & Paula Oliver Llorente, *The Digital Economy and the New Social Contract*, IE University Center for the Governance of Change, https://www.ie.edu/cgc/research/new-social-contract-digital-age/, visited on 15 May 2026.

进创新，并为成功提供平等机会；二是个人将信任组织能够负责任地处理其个人数据；三是社会将更加繁荣，从而改善整体福祉。[55] 他们认为数字社会新问题不能仅靠技术来解决，而应当重构社会运行结构，构建新社会契约，并提出了四项核心建议：合法性、多利益相关方合作、公共部门转型和私营部门参与。[56]

其次是数字自决理论。韦尔胡尔斯特教授试图构建一套实现数据社会化重用的数据治理理论。他认为，个保法未触及重用问题，现行的数据治理也缺乏对数据重用的关注。跨领域的数据分享需要社会许可，使负责任的数据使用延伸至数据重用。[57] 当前解决信息和权力不对称的方法是知情同意，而在数据化时代，知情同意原则已不足以支撑数据重用。[58] 因此需要超越同意的局限性，寻找支撑更全面、更包容、更负责任的数据使用和重用的理论基础。为此韦尔胡尔斯特教授提出新的数字自决原则和实践，并将之定义为“在整个数字数据生命周期中以互惠互利的方式尊重、嵌入和执行人们的代理、权利、利益、偏好和期望的原则”[59]。其中，社会许可是实施数字自决的政策工具，为整个行业建立实践标准，有助于促进负责任的数据重用。于是，韦尔胡尔斯特在寻求超越个人同意实现新的负责任治理体制中提出社会许可或社会契约理论，以可持续、公平和负责任的方式释放数据的力量。[60] 社会许可可以通过与社区、利益相关者和更广泛的公众接触、谈判并获得他们的信任和接受来获得。[61]

最后，数据民主理论也支撑社会契约理论的应用。数据民主[62]的理念强调数据应该被每个人访问、理解和使用，体现了数据处理中的包容性、透明度和问责制原则。数据民主的理想是“数据的好处由所有人共享，数据驱动的创新服务于人类的集体利益”[63]。显然，数据民主理论强调使用者有机会获取数据，同时也强调个人通过参与和合作分享数据好处。

上述三种理论相互交叉和联系，超越了仅关注数据主体权利的个保法理论，转向通过社会主体参与集体协商方式形成新的数据获取和使用秩序。

（二）社会契约适用的正当性论证

社会契约理论起源于霍布斯、洛克和卢梭等先贤对民主政府权力来源或正当性的论述，之后

---

〔55〕 See *Towards a Fair Data Economy: Key Lessons from Finland on Building a National Roadmap*, IE University Center for the Governance of Change, https://www.ie.edu/cgc/research/new-social-contract-digital-age/, visited on 15 May 2026.

〔56〕 Otero-Iglesias & Llorente, supra note〔54〕.

〔57〕 See Simona Marcucci, Natalia G. Alarcón, Stefaan G. Verhulst & Elena Wüllhorst, *Informing the Global Data Future: Benchmarking Data Governance Frameworks*, 5 Data & Policy e30 (2023).

〔58〕 See S. G. Verhulst, L. Sandor & J. Stamm, *The Urgent Need to Reimagine Data Consent*, Stanford Social Innovation Review, 2023, https://doi.org/10.48558/TDS9-6Y22, visited on 15 May 2026.

〔59〕 Verhulst, supra note〔30〕.

〔60〕 Verhulst, Sandor & Stamm, supra note〔58〕.

〔61〕 到目前为止，已经尝试了几种不同的参与式方法，以实现更具包容性和民主的数据重用治理。其中包括：审议性讨论小组、圆桌会议、公民陪审团和调查、公民集会、建立数据（再）使用社会许可实验室等。Ibid.

〔62〕 数据民主是一种组织状态，员工可以定期和普遍地（1）访问数据资产，（2）利用它们的技能，（3）具有参与其中的动机以及（4）战略性地使用它们的指引。See Nick Van Der Meulen, *Mobilize Your Data Democracy*, MIT CISR, 18 September 2025, https://cisr.mit.edu/publication/2025_0901_DataDemocracy_VanderMeulen SomehWixomBeath.

〔63〕 Ankit Raghuvanshi, *Understanding the Need for Data Democracy in the Digital Age*, 9 (6) International Journal of Novel Research and Development (IJNRD) e245 (2024), https://www.ijnrd.org/papers/IJNRD2406421.pdf, visited on 15 May 2026.

罗尔斯则更新了社会契约论，将社会契约理论的范围扩展到社会正义和道德规范理论，大大丰富了社会契约的内涵。社会契约理论并没有告诉人们社会安排是如何设计的，而是强调赋予个人同意、协议和谈判的重要作用。权威学者将之表述为："规则是由理想化的个体 N 在某种理想环境 M 中选择的，遵守规则的义务适用于 N（真实的个人）。"[64]因此，社会契约可以理解为关于社会基本规则的协议，而社会契约理论主张这样的规则应该不断重新谈判、更新和完善，以实现社会成员共同认可的目标。按照罗尔斯的理论，正义是社会安排的主要美德，如果人们合作选择的程序是合理的，那么合作安排就符合我们的道德判断，具有公平性或合法性。

在笔者看来，社会契约论是一种方法论，可以广泛地应用于"个人为了社会利益而将一些自由交给治理实体"的情形，用来解释相冲突的利益相关者如何在合作过程中通过动态互动寻求各自利益的最大化，如何在相互让渡权利和约束条件下实现符合参与者个体利益的稳定均衡。数据上存在多重利益，数据资源化利用必须解决这些利益冲突，构建数据使用秩序，实现数据社会价值最大化。因此，社会契约理论适合数据使用和重用秩序构建，以寻求数据的社会化使用规则。从社会契约视角，数据使用或重用的规范和规则的合法性最终来自对个人产生合理期望的认可或社会共识。

传统个保法认为，只要基于个人同意，使用者的使用行为就具有正当性，也具有合法性。[65] 这也符合传统的社会契约理论。但当我们的同意并非出于自愿，不能反映个体意志时，同意就不具有正义可言。而社会契约理论讨论的是制度规则的道德合法性。[66] 当代社会契约理论的核心思想是协议（agreement），而不是同意（consent）。同意区别于协议，一个人可以认可或同意一项原则，而这种认可行为并不以任何方式约束他必须遵守，而协议行为表明了我们有什么理由做什么。[67] 从当今社会契约理论的角度，将个人在具体场景下同意使用视为当然的合法，其合理性就存在疑问。

在我们重构个人数据使用秩序时，可以借助社会契约理论寻求新的正义。韦尔胡尔斯特将社会许可定义为"通过持续（即不断更新）的社区或利益相关者参与，以及对数据访问和重用方式的接受，来建立信任和合法性的过程"[68]。他的社会许可本质上就是在援用社会契约理论，寻求实现数据重用的新的社会正义。在某种意义上，同意作为合法性基础是个保法立法者们基于当时社会背景设计的正当性，但正当性内生于合理的协议。[69] 当我们需要重新思考个人数据的社会化利用秩序时，社会契约理论恰为这一重构提供了可行路径。

（三）社会契约引导的个人数据治理模式探索

社会契约理论引导人们重新思考和探索数据主体（个体）为了社会利益应当让渡自由（权利）的内容、范围和程度，形成新的既有效保护个人，又最大化实现数据社会化的使用（重用）秩序。它要实现从个体意志到集体或社会意志的跃迁，在结果上表现为社会契约（社会许可）；在过程上，

---

〔64〕 Fred D'Agostino, Gerald Gaus & John Thrasher, *Contemporary Approaches to the Social Contract*, The Stanford Encyclopedia of Philosophy (Spring 2024 Edition), https://plato.stanford.edu/entries/contractarianism-contemporary/, visited on 15 May 2026.

〔65〕 参见孙莹：《论已公开个人信息合理处理范围的认定》，载《法律科学》2025 年第 6 期。

〔66〕 道德合法性涵盖了社会合法性（该制度实际上是否被广泛接受?）、地方价值合法性（制度是否具有符合当地期望和价值观的属性?）和整体道德合法性（从所有方面考虑，该制度在道德上是否可接受?）。See Hugh Breakey, Graham Wood & Charles Sampford, *Understanding and Defining the Social License to Operate: Social Acceptance, Local Values, Overall Moral Legitimacy, and "Moral Authority"*, 102 Resources Policy 105488 (2025).

〔67〕 D'Agostino, Gaus & Thrasher, supra note〔64〕.

〔68〕 Verhulst, Sandor & Stamm, supra note〔58〕.

〔69〕 D'Agostino, Gaus & Thrasher, supra note〔64〕.

体现为个体参与规则形成和实现的体制。

从某种意义上，数据信托即一种基于个人意志的个人数据集成管理利用的制度。目前，人们提出了两种克服信托缺陷的解决方案：社区参与模式和公共信托模式。韦尔胡尔斯特教授是社区参与模式的倡导者。他认为，当前数据使用治理失败的原因是同意疲劳、溯源薄弱和许可不平衡，因而转向集体和公平的数据治理，需要一种持续、可执行的参与式数据治理机制。数据治理被视为一个集体的、持续的过程，将重点从个人同意转移到社会决策。[70] 社会许可的形成大致可以归纳为三个核心阶段：(1) 建立偏好和期望；(2) 偏好和期望的条款化；(3) 执行偏好和期望。[71] 与单纯的法律合规不同，社会许可嵌入了社会信号、偏好和对目的、保障、监督和问责制的期望，因为数据在不同环境中被重复使用并不断发展。[72]

但是，真正的社会许可实施需要一定的条件，至少利益相关者和公众参与是一个难以解决的问题。芝加哥大学的胡克(Aziz Z. Huq)教授探讨了“公共信托”作为个人数据治理新模式。他认为，公共信托是对共同资源进行民主决策的工具，同时解决了私人和公共滥用的风险。个人数据作为一种共享资产，可作为为所有人利益而共同持有的资产进行管理。[73] 公共信托资产由国家拥有和管理，国家作为受托人既可以为公众的利益保留或限制使用，也允许实控人用于受控的商业开发。本质上，公共信托作为个人数据的治理工具，为政府监管个人数据使用提供依据，以减轻个人数据使用的危害，实现平等保护公众隐私和经济利益的目标。

在智慧城市建设过程中，美国、欧洲和加拿大的市政当局已经开始尝试对数据进行有限形式的公共信托。[74] 阿姆斯特丹与巴塞罗那和纽约市共同发起了数字权利城市联盟，[75]探索公共信托模式的实现路径。

虽然上述两种模式都是替代现行个人同意，实现个人数据社会化使用，但是二者理论基础不完全相同。基于社区参与的社会许可以个人自主权为基础，只是从个体决策(同意)转向更民主的集体决策；公共信托模式则基于数字公平理论，希望由政府管理和监督个人数据的社会使用，强调政府的代理人作用。笔者认为，保护数据主体的正当权益是基本共识，在这方面个保法仍然发挥着作用。我们应当在个保法框架下思考新社会契约，可以考虑从重构合法性基础的角度更新个保法方案。

五、个人数据治理的模式更新与制度回应

个保法采用“合法性基础＋处理行为规范”的行为规范模式，但其个人自决的理论基础导致个

---

〔70〕 See Stefaan G. Verhulst, Adam Zable, Andrew Zahuranec & Peter Addo, *Reimagining Data Governance for AI: Operationalizing a Social License for Data Re-Use*, Agence Française de Développement, 28 April 2025, https://www.afd.fr/en/ressources/reimagining-data-governance-ai.

〔71〕 Stefaan G. Verhulst & Adam Zable, *A Facilitator's Guide to Establishing a Social License for Data Reuse*, The Living Library, https://thelivinglib.org/a-facilitators-guide-to-establishing-a-social-license-for-data-reuse/, visited on 15 May 2026.

〔72〕 Ibid.

〔73〕 See Aziz Z. Huq, *The Public Trust in Data*, 110 Georgetown Law Journal 333, 333－402 (2022).

〔74〕 Ibid.

〔75〕 数字权利城市联盟(Cities Coalition for Digital Rights)被视为一项正在进行的全球倡议，旨在促进和捍卫城市和城市环境中公民、居民和游客的数字权利，以确保公平、包容、可访问和负担得起的非歧视性数字环境。截至2026年2月大致有60家城市加入该城市联盟。Cities Coalition for Digital Rights, https://citiesfordigitalrights.org, visited on 15 May 2026.

人控制是其基础底色。个人控制体现于“处理前个人同意＋处理中干预＋处理后删除”，这是在事实上为个人构筑完整权利链，使个人在法律上享有资源化利用的话语权。但是，以“目的特定＋个人同意”配合构建的个保法体系正在崩塌。其根本原因并不在于初始个人保护的理念和制度设计是错误的，而是因为技术变革带来的数据要素利用方式变革对法律制度提出新需求，同时也使传统的以个人控制为基础对个人保护的方式失效或失灵。2018 年笔者曾撰文指出个人信息保护应从个人控制走向社会控制，并提出社会控制的三层含义：个人信息的使用由社会习惯或法律确定，而不是由个人意志决定；保护个人信息的责任主体由以个人为主转向以社会为主；法律规范的重心应从收集行为转向使用行为。[76] 在今天看来这些主张仍然是合宜的且适合人工智能时代的数据利用需求。本文承继这一思路，提出以社会契约重构个保法的合法性基础。也就是说，个人数据的收集和获取不再事先获取个人同意，而应在法律上视为所有个人默许收集使用，但是个人数据使用须实质性地尊重和保护个人权益。

（一）社会许可下的个人数据处理合法性重构

为解决数据要素化使用与个人控制之间的冲突，我们需要构建新的合法性基础，并更新和修改个人数据使用（处理）规范，实现个人保护和社会使用的平衡。为此，笔者建议以社会许可替代个人同意，作为个人数据处理的合法性基础，并在此基础上适当修改调整个人与使用者之间权利义务的处理规范，实现更新个保法的目标。

社会许可，是指基于其与社区价值观和利益的一致性，对数据重用等活动的集体接受。[77] 作为个人数据使用合法性基础的社会许可，即社会中的每个人都允许个人数据使用，或者接受使用个人数据不需要每个个体同意，只需要遵守法律规定，合法获取和使用数据。至此，全社会形成共识，只要使用者以合法方式获取和使用数据，且用于合法正当的目的，那么每个人都默示同意。默示同意替代个保法的积极同意制度，数据使用者不需要在收集时征得同意，之后也不需要重新取得同意，在供他人使用时也不需要单独同意。

在法律上，社会许可类似于版权法的开放许可[78]，即毋须获得特定数据主体个体的明确同意，只要遵循标准开放许可条件就推定使用者愿意遵守该许可使用数据。社会许可的开放性体现为两个方面：一是主体开放性，社会许可是向所有主体开放的；二是社会许可的内容或条件也是开放的，不再受特定目的约束。这样，社会许可就摆脱了目的特定原则对个人数据重用的限制。不过，这种使用存在三个限制条件：一是获取个人数据的手段和方式合法；二是遵守个保法的规定，履行保护数据主体权益和其他法定义务；三是用于正当合法的使用目的。上述三个条件中，合法目的是最宽泛的授权，允许个人数据用于任何合法目的或用途，以突破目的限定原则。以这样宽泛的合法性为基础是否具有法律上的正当性，需要进一步检讨。

《个保法》第 13 条的合法性基础采意定和法定二分，要么基于个人同意，要么基于法律规定的事由。两者的正当性（合法性）是建立在不同法理基础之上的：同意的合法性基础是个人自主决定（同意），而法定事由显然是从社会理性角度的推定或假设。这些法定事由或情形的正当性可以归纳为三

---

〔76〕 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。

〔77〕 See Stefaan G. Verhulst, *Beyond Checking a Box: How a Social License Can Help Communities Benefit from Data Reuse and AI*, TechXplore, 16 December 2024, https://techxplore.com/news/2024-12-social-communities-benefit-reuse-ai.html.

〔78〕 开放许可源自版权许可，通常由版权管理协议适用于可开放使用的受版权保护甚或不受版权保护的资源。开放许可有以下特征：许可使用的条件是标准化的，凡使用者均适用；受许可人不受限制，只要遵循许可使用条件的人即可以获得许可或使用；许可使用的客体限于软件、研究数据等非排他可重用数字内容。

类：(1) 订立、履行合同所必需，因为个人信息是订立和履行合同所必需的，是实现个人目的所必需的；(2) 已公开个人信息原则上可在合理的范围内使用，因为已公开信息被推定为基于个人意志或个人不再控制；(3) 其他法律规定的允许在合理的范围内处理个人信息的情形，[79]是指满足特定的公共利益、公共安全目的或属于好意施惠，这些情形是社会主义核心价值观所提倡的，为社会秩序所必需，是个人必须让渡的自由。前两类免于同意事由再加上好意施惠情形，似乎是从社会常识推演而得出的，其本质具有社会契约性质；而其他事由是法律理性的结果，它基于个人与社会公共利益之间发生冲突时个人必须做的妥协，当然具有法律的正当性。因此，第 13 条法定事由规定实际上反映了社会认知和共识，具有转化为社会契约的正当性。

第 13 条法定情形是开放式规范，“法律、行政法规”还可以比照之前事由来规定的“其他情形”下同意的豁免。若我们将合法性基础替换为默示“合法正当目的”，不仅可以涵盖法定事由，而且可以反映出个人信息正当使用事由的开放性。因此，只要目的合法正当，均可以作为获取并使用个人数据的正当理由，这与当前合法性基础的制度逻辑并不存在根本冲突。当然，从立法技术出发，亦可以从禁止性规范的角度，通过列举不得(非经同意)使用个人信息的情形，以排除开放许可下对个人有实质危害的使用。

在上述限制条件下，社会许可可以替代同意并吸收法定事由成为唯一的合法性基础。这样可以避免烦琐的同意流程，使需要数据者可以获得个人数据加以使用，解锁重用之困，使数据价值得到发挥。但是，实施开放社会许可，个人既不能决定使用条件、范围和方式等，也无法明确特定使用者或使用关系，可能增加个人数据处理危害个人权益的风险和维权困难。因此，适用开放许可对于基于个人同意的个人保护水平有一定程度减弱，因而需要通过其他制度来加以弥补。毕竟只有个人数据权益没有减弱甚至得到增强的条件下，才有可能实现实质性保护个人和促进利用的双重目标。

(二) 社会许可下的个人数据治理规范更新

在社会许可下，现行个保法的个人数据处理规范需要进行相应调整，基本方向是：直面人工智能普及应用对个人保护的新挑战，实质性地保护个人在个人数据使用中的正当权益，在给数据使用者更多自由的同时，强化个人在数据处理中的义务和责任，构建负责任治理体系。本文仅对此作方向性的论述：

1. 重塑个人的正当性权益

在现行个保法中，个人被赋予相当多的防御性权利，这些权利大多数属于沉睡中的权利，人们也并未真正行使。在弱化个人数据使用由个人控制的理念下，数据主体应当保留和享有哪些权利值得进一步明晰和重构。除了原则性宣示个人对个人数据及其使用享有主体权利外，笔者认为，可以保留知情权和拒绝(选择退出)权两个基本权利，同时增加收益分享权并细化损害赔偿救济的规定。

个人数据使用存在直接收集和间接获取(包括爬虫抓取公开信息等)两种方式。在直接收集时，使用者仍然需要告知个人，个人仍然需要勾选，只是勾选不再赋予同意(甚或授权)效力，仅作为知晓谁在使用其个人数据的证明。在间接获取的情形下，获取时无法告知，可以将告知延迟到使用过程中识别主体身份之后(一旦进行识别性使用，告知数据主体成为使用者法定义务)。在使用关系得以建立的情形下，法律可以规定一些特定的数据使用情形(典型的如精准推送、敏感信息使用等)须给予数据主体以拒绝机会，防范数据使用侵犯个人隐私和其他权益。

---

[79] 《个人信息保护法》第 13 条第 1 款第 3 至 5 项：(三) 为履行法定职责或者法定义务所必需；(四) 为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；(五) 为公共利益实施新闻报道、舆论监督等行为。

在数据资源化利用下，个人数据聚合利用给使用者带来价值，作为个人数据提供或参与生成者的个人有权分享由此产生的经济利益。因此，应当明确数据主体的收益分享权。收益分享权也可以视为对数据可携权的替代，[80]它不再是通过数据控制权来实现利益，而是直接代之以收益权。一旦在具体数据使用关系中收益权得不到实现，那么数据主体可以请求特定使用者分享因数据聚合使用产生的利益，在不能实现时通过司法救济实现。这样的数据收益分享实践可以促成各种数据合作方式的开展，以形成数据主体参与治理和分配的治理模式。

2. 强化使用者的法定义务

在个人数据使用的合法基础调整之后，如何完善个人数据处理规范，强化使用者保护个人权益和履行合规义务便成为个保法主要目标。在这方面除了细化安全保障义务之外，可能有三个方向需要强化：

第一是告知义务。告知是实现数据主体知情和行使权利以及维权的基础，因此，细化和完善告知义务成为保护个人权益的前提。一个基本原则是：凡是使用个人数据的，均须履行告知义务，无论直接收集还是通过间接方式获取，都应当与数据主体建立联系。

第二是正当合法使用个人数据的义务。这是开放社会许可的基本要求，因此期待法律对合法获取方式、违法使用情形及其法律后果作出更细致的规定，以发挥对合规者的指引作用和对违法者的惩罚作用。

第三是保护个人权益的义务。个人对个人数据及其使用的合法利益需要通过使用者义务来实现，因此除了使用者具有保护个人合法权益义务的原则性规范外，更需要细化这些保护义务，以使个人通过侵权和违法救济获得保护。例如保护隐私和敏感信息、分享数据利益等义务。

3. 构建负责任的治理框架

个人数据在使用中产生价值，也在使用中产生损害和风险，个保法在具体场景下执行，需要结合具体场景判断合法性，以及预防措施与风险的适当性。这需要组织建立有效的治理体系来解决。如前所述，在美国，无论学术界还是政策制定者均认可个人保护应当从以个人权利为中心转向负责任使用的治理体系。个人数据及其使用是一个持续、多变、复杂的存在，个人与使用者、监管者与使用者之间存在着巨大的信息不对称。法律规范的完善需要落实到每个组织治理体系，需要使用者建立全流程合规管理来落实法律义务，切实维护个人权益。个人数据治理在某种意义上需要在社会层面形成共识和最佳实践，由各组织因地制宜落实和实施。在这方面，国际社会已在研讨下一代数据治理，汇聚技术、法律和社会领域的研究人员以及行业专家，共同探讨数据治理可行方案。[81] 这样的治理体制反映了数据智能时代的趋势，应当成为未来个保法不可或缺的内容。

4. 完善损害赔偿救济体系

个人与数据使用者之间只是在收集环节减少了所谓的“同意授权”，但是并不减少数据使用者保护数据主体权利的义务，法律仍需强化救济体系来实现对个人权益的保护，这是转向负责任地使用的治理体制的配套制度。数据保护具有复杂性、广泛性，既有对个体的损害（财产损失、人身

---

〔80〕 数据可携权允许个人从使用其个人数据所创造的价值中受益：它允许他们将数据用于自身目的，或许可数据进一步用于第三方以换取额外服务或现金价值。参见付新华：《数据可携权的欧美法律实践及本土化制度设计》，载《河北法学》2019 年第 8 期。

〔81〕 例如 2024 年 9 月 17 日，下一代数据治理研讨会（NeXt-generation Data Governance workshop）在阿姆斯特丹召开。See NeXt-Generation Data Governance Workshop, Amsterdam, 17 September 2024, https://nxdg-workshop.github.io/2024/.

伤害、歧视、心理伤害等），也有对整个社会的损害。[82] 人工智能的广泛应用又会加剧数据导致损害及其责任追究的复杂性。在索罗夫看来，仅凭数据本身无法确定任何有意义的监管措施，隐私法必须关注使用中的损害和风险，而非个人数据的性质，数据保护措施应与数据收集、使用和转移所涉及的损害和风险相称。[83] 因此，未来的个保法将朝着完善个人数据使用规范和损害赔偿救济体系的方向发展。

在强化损害赔偿救济的同时，还需要强化个人数据使用监督和执法，打击一切违法利用个人信息、侵害合法权益、危害公共秩序和国家安全的行为，发挥行政执法、刑事司法和社会综合治理的作用。只有营造合规合法使用个人信息的环境，才能减少个人数据使用带来的不安全感。

总之，合法性基础的开放性规范需要整个数据使用规范作相应调整和更新，在抛弃形式化同意制度之后，建立更加完善和有效地保护个人权益（和整个社会）的制度。同时，将个人数据的社会使用交由使用者决定，释放数据社会化重用的价值。这样，个保法就彻底地从基于个人权利的法律转变为行为法，一切违法性判断均依据单一法律规范作出判断，避免个人决定（同意）对违法判断的干预，同时也避免个人决定对正当数据的重用设置障碍（至少是增加合规成本）。

六、结　　论

数字技术不断迭代使人类社会进入数智时代，个人数据应用的目的、方式、场景、规模等发生了巨大变化，一方面导致个人对个人数据的控制力越来越弱，另一方面导致社会（由各使用者组成）越来越依赖数据的重用，迫切需要建立高效便捷的数据社会化重用秩序。但是，20 世纪七八十年代所形成的个人数据保护制度尚未预料到个人数据资源化利用方式的变革，更没有给个人数据社会化重用提供机会。因此，个人数据保护与资源化利用存在着制度冲突。

应当说，自互联网、大数据出现后对于个保法的反思和改革的思考从来没有停止过，只是因为路径依赖没有一个国家能够实现实质性改革，而人工智能的出现，彻底地粉碎了以“个人决定”为核心的个保法制度。个人在个人数据及其使用中主体权益与数据（作为资源）社会化重用之间存在冲突，不得不通过体系性变革加以解决。社会契约理论无疑提供了强有力的理论支撑，而域外学者主张和行业探索也给了我们有益的启迪。本文认为，个人数据使用（重用）需要秩序，但是欧洲开创的以个人控制为核心的个保法模式使得个人同意渗透或延伸至数据资源利用秩序，构成个人决定（同意）与使用者决定之间的紧张关系。这种紧张关系在我国《个保法》中得到强化，形成了个保法与数据要素化（资源化）利用的冲突，单独同意尤其成为个人数据流通的阻碍。鉴于个保法以“合法性基础＋处理行为规范”为架构，我们只需对以个人同意为基础的合法性基础予以完善，并更新个人数据处理行为规范，即可实现个保法与时俱进的立法目标。

因此，本文提出以社会许可来替代同意及其他法定事由，构成开放的个人数据使用的合法性基础，更新和完善个人数据使用（处理）规范，以实质性地保护个人在个人数据使用中的正当权益，在给数据使用者更多自由的同时，强化个人数据处理中的义务和责任，构建负责任治理体系。最

---

〔82〕 Information Commissioner's Office, Overview of Data Protection Harms and the ICO's Taxonomy, April 2022, https://policycommons.net/artifacts/3331588/overview-of-data-protection-harms-and-the-ico-taxonomy/4130440/, visited on 15 May 2026.

〔83〕 See Daniel J. Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 Northwestern University Law Review 1081, 1081 - 1138 (2024).

终使个保法彻底转变为行为法，使个人数据的资源化利用由使用者决定。与此同时，数据使用者负担维护个人对个人数据及其使用的合法权益的义务。这样的改革方案受到社会契约理论的鼓舞，因为它试图重新寻求数智时代个人数据使用（重用）正当性或合法性。但笔者没有主张通过社区参与和重新谈判来达成新正义或新秩序，而是基于法律理性主张，在保护个人信息权益的前提下，社会应当默认或一致同意个人数据正当使用行为。这样的方案充分考虑到不管数字技术如何发展，我们仍然需要个保法，需要更加完善和有效的个保法来保护数据主体权益。因此，笔者的方案可以视为个保法修改方向的建议，即以社会许可替代现行法的合法性基础，并修改和完善个人数据处理（使用）规范，以实现体系化更新个保法的目标。

Abstract　With the iterative development and deep application of digital technology, "data+AI" has been driving continuous social change. How to unleash the value of data while fully protecting the rights and interests of all parties has become a hard nut to crack in various countries. The utilization of data resources (or as a factor of production) requires the social reuse of data, which means that data is available and users have the right to decide how to use it. However, there is a structural tension between the current personal data governance system based on individual decisions and the practical need for data resource utilization. Therefore, European countries and the United States are actively exploring institutional reform that meets the needs of the times. Among them, the United States continues to improve its "responsible data governance" system, while Europe expands the scope of "legitimate interests" through law amendments and moderately relaxes compliance supervision to respond to the institutional challenges brought about by the resource utilization of personal data. In the exploration of institutional restructuring, social contract theory has been introduced into the field of personal data governance, providing a new theoretical perspective for re-examining the allocation of rights and institutional arrangements between individuals and society in personal data governance. Specifically, the lawful basis (legitimacy foundation) should be reconstructed based on the social license mechanism, and corresponding adjustments should be made to the rights and obligations between data subjects and data users. These changes will help the Personal Information Protection Law to transform from the "entitlement law" to "action governing law", thereby resolving the institutional conflict between personal protection and resource utilization, and achieving the dual goals of protecting the rights of data subjects and promoting the social reuse of data.

Keywords　Personal Data, Personal Data Governance, Personal Decision-making, Social Contract Theory, Social License

（责任编辑：曹博）