法商研究 Studies in Law and Business
Vol. 37 No. 2 (2020)

数据驱动时代的数据隐私保护

——从个人控制到数据控制者信义义务

解 正 山*

摘 要:在数据驱动时代,个人数据隐私引发广泛的担忧。基于个人具有隐私自我管理能力的假定,立法者建构了一套沿袭传统个人主义隐私观的数据隐私保护法律框架。这种强调个人控制的立法取向高估了个人在数据实践中的自治能力,难以应对数据时代的隐私挑战。可考虑将信义义务引入新型的数据关系之中,要求自动驾驶汽车制造商、其他智能交通服务提供者以及数据驱动的其他商业场景中的数据控制者以数据受托人身份管理或处分其占有的个人数据,强化其数据受托职责,以弥补个人在隐私管理中的能力不足。

关键词:数据隐私 个人控制 数据受托人 信义义务

最近几年,大数据及移动互联技术掀起了新一轮全球技术革命浪潮,万物互联时代或将不期而至。其中,自动(无人)驾驶汽车最受瞩目并成为各国汽车产业技术变革与转型升级的突破口与战略制高点。传统车企与互联网巨头正在将只在科幻电影中出现的自动驾驶汽车变为现实,深刻影响着人们的出行与生活方式。一方面,高度智能的自动驾驶汽车具有显著的经济与社会效益,如减少人为错误导致的交通事故、提高交通效率等。但另一方面,除带来致害责任归责、网络安全等法律难题外,数据驱动的自动驾驶汽车还将引起用户(亦称数据主体或消费者)对其隐私的担忧:谁在采集个人数据(个人数据一般指可识别具体个人的任何信息,其与个人信息具有内在的一致性,本文不加区分地使用这两个称谓)?这些数据是否会被不公平或不当地使用?如何控制个人数据的采集与使用?促进技术创新与数据隐私保护是否不可调和?这些问题清单着实恼人,且在数据驱动的其他商业场景中同样存在。鉴此,本文以即将商用的自动驾驶汽车为切入点,对上述问题进行探讨。

一、数据驱动下的隐私挑战:以自动驾驶汽车为切入点

目前,正在测试中的自动驾驶汽车分别运用了传感器技术与连通性技术:前者主要依托车辆自身配置的立体摄像机、雷达等先进传感器采集车辆安全运行所需的内部操作与外部环境数据,而后结合

* 上海对外经贸大学法学院副教授

执行器、控制单元以及集中软件等对周围交通环境变化进行监测并作出反应;后者则通过无线短距通信技术实现车与车、车与交通基础设施以及车与人之间的实时连通,确保自动驾驶汽车即时从外部获取事关安全驾驶所需的交通环境数据,包括共享网络的其他车辆或行人的状态信息、定位数据、交通信息等,同时它自身的内部状态数据也将通过网络自动传送给附近的网联车辆或共享网络的使用者。① 不难看出,自动驾驶功能的实现离不开大规模的数据采集与使用。这些数据不仅包含技术改善与安全驾驶等方面所需的信息,而且还包括超出驾驶之外且与个人喜好有关的浏览历史、导航历史以及广播收听历史等大量信息。尤其是,随着生物识别以及视频追踪等新技术应用于自动驾驶汽车,用户嗓音、心率、指膜等生物信息也都可能被采集。最终,自动驾驶汽车不仅有能力收集其想要获得的任何数据,而且还能存储这些数据并将它们上传到车外的数据服务器以备未来之需。②

自动驾驶汽车可记录并提供过往以及实时的位置数据,包括驾车时间、行车路线、访问地点、目的地等较具敏感性的数据。虽然这些位置数据不足以直接识别出某个自然人,但若将它与其他数据结合进行相关性分析,那么对这个人进行"画像"就变得可能了。由此,自动驾驶汽车的用户们自然担心事关他们健康、职业、个人品行、政治或宗教信仰等敏感信息暴露于被他人窥探的风险之中,最终导致自己成为他人眼中的"透明人"。更常见的隐私挑战是,自动驾驶以及数据驱动的其他商业场景中的数据采集者、处理者或使用者(以下统称数据控制者)对用户的消费操控或诱导。通过追踪用户经常光顾的店家、日常活动或饮食习惯,数据控制者将能识别出这些潜在消费者的个人偏好、购买模式甚至生活方式,从而进行精准的市场推广或广告投放。这种"数据画像使得定向广告无比精准地在特定时间和场景达到目标客户,诱发冲动消费……这不啻是一种消费操纵",③难免会侵犯用户的自主且有损他们的尊严。自动驾驶汽车还将产生一些与位置或目的地无关的数据,如能反映用户驾驶习惯的车辆速度、制动模式等数据。用户对这些数据同样有强烈的隐私期待。其实,对数据控制者而言,是否掌握足够能识别某个具体个人的数据已不再那么重要,大数据分析技术已使这些数据驱动的商业机构仅凭数据相关性而非因果关系即可进行预测与推断,而用户很多时候对此却一无所知。可见,对用户而言,真正的挑战是:数据采集、处理及利用多以他们看不见的方式进行,即使他们怀疑自己的隐私受到侵害,可能也无法确定谁是加害者,或缺乏必要的证据证明自己的实际损害和侵权者的责任;而且,用户接收广告时可能根本就没有意识到这是预测性广告,更不用说自己的哪些行为、哪些数据被收集和分析了。④

尤令人担心的是,一些敏感的个人数据可能被用于对个人进行不公平的推断,特别是当现有数据库本就对某些种族或性别的人存有偏见时,就可能进一步加剧现存的社会不平等现象。⑤ 正如我们所知,大数据分析已使数据控制者具备超乎想象的预测能力,这对数据主体未来的借贷、工作、旅行、

① See Jeffrey K. Gurney, Driving into the Unknown: Examining the Crossroads of Criminal Law and Autonomous Vehicles, 5 Wake Forest Journal of Law & Policy, 393－400 (2015).

② See Emilio Longoria, Invisible, but Not Transparent: An Analysis of the Data Privacy Issues That Could Be Implicated by the Widespread Use of Connected Vehicles, 28 Albany Law Journal of Science & Technology, 8－9 (2017).

③ 叶名怡:《个人信息的侵权法保护》,《法学研究》2018 年第 4 期。

④ 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。

⑤ See Hazel Si Min Lim et al., Autonomous Vehicles for Smart and Sustainable Cities: An In－depth Exploration of Privacy and Cybersecurity Implications, 11 Energies, 1062－1084(2018).

获得住房、接受大学教育等都可能产生显著影响,[①]尤其是基于分类筛选形成的"大数据黑名单"将导致某些特定群体或个人丧失或被限制行使部分权利或机会,如数据控制者利用掌握的数据并据此预测数据主体未来罹患严重疾病的风险,进而拒绝向其提供工作机会、住房或贷款。加之"算法黑箱"以及数据泄露或买卖使得上述分类筛选与歧视得以秘密化和便利化,以至于那些被列入"黑名单"的当事人很多时候既无从知晓亦无法摆脱。[②] 所有这些无不表明,若无适当的隐私保护机制,个人数据被滥用或将层出不穷,这不仅会加剧社会歧视,也将影响信息社会的可持续发展。

一直以来,汽车都被认为是自由与个人自主的象征。然而,自动驾驶汽车与外部环境自行互动很可能使用户自主受到某种程度的限制。尤其是,当自动驾驶汽车的路线全部或部分受控于集中的政府网络时,人们势必担心自身隐私尤其是自主权受到损害。[③] 这种担心并非空穴来风,因为在技术上完全可能。因此,有评论者不无忧虑地指出,人们喜爱汽车是因为他们能控制这种强大的机器,一旦方向盘与脚踏板不再必要,驾驶的乐趣就将随之丧失,那些热衷于汽车象征性与情感性价值的消费者群体将因此抵制这种新产品。[④] 此种担忧虽不无道理,但并非不可解决。例如,为保护用户的自由与个人自主,美国加利福尼亚州与内华达州关于自动驾驶的法律规定,一旦用户提出要求,自动驾驶汽车应将驾驶控制权交给用户。

真正的问题在于,自动驾驶汽车能精确记录用户大量的公开活动数据,且这些数据蕴含着他们的家庭、政治、职业、宗教以及生活等诸方面的丰富细节,如果数据控制者收集个人数据的权力不受限制,自动驾驶汽车就将为数据监控提供便利甚至成为大规模远程监控的平台,[⑤]个人的隐私空间将因此受到影响或侵害,就像全景式监狱里的囚犯,即便不知道是否有警卫站岗警戒,也会因为害怕被监视而改变各自的行为。[⑥] 进一步而言,即便数据采集都是合法的,但鉴于如此丰富而全面的数据足以让数据控制者对车辆用户进行"画像",因此这些消费者定会担心他们受到这些数据采集机器的"监视",从公共关系角度看,这显然令人难以接受。[⑦] 人们甚至担心,智能网络控制者可能会利用其所掌握的路线选择权之便利,向那些愿意使用更快路线并支付相应对价的用户优先提供服务,而普通用户将被迫使用较慢路线。与其说这是个人自主问题,倒不如说是交通公平的问题。这或将带来一个更不公平的社会或造成更大的社会不安,智能化的城市治理将因此遭遇挫折。[⑧]

---

① See Danielle K. Citron & Frank Pasquale, the Scored Society: Due Process for Automated Predictions, 89 Washington Law Review, 18 (2014).

② 参见叶名怡:《个人信息的侵权法保护》,《法学研究》2018年第4期。

③ See William J. Kohler et al., Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles, 31 Santa Clara Computer High Technology Law Journal, 123 (2015).

④ See Jack Boeglin, the Costs of Self-driving Cars: Reconciling Freedom and Privacy with Tort Liability in Autonomous Vehicle Regulation, 17 Yale Journal of Law and Technology, 178 (2015).

⑤ See Joshua Schoonmaker, Proactive Privacy for a Driverless Age, 25 Information & Communication Technology Law, 96 (2016).

⑥ See Jack Boeglin, The Costs of Self-driving Cars: Reconciling Freedom and Privacy with Tort Liability in Autonomous Vehicle Regulation, 17 Yale Journal of Law & Technology, 183 (2015).

⑦ See Chasel Lee, Grabbing the Wheel Early: Moving Forward on Cybersecurity and Privacy Protections for Driverless Cars, 69 Federal Communication Law Journal, 33 (2017).

⑧ See Hazel Si Min Lim et al., Autonomous Vehicles for Smart and Sustainable Cities: An In-depth Exploration of Privacy and Cybersecurity Implications, 11 Energies, 1062-1084(2018).

综上可见,自动驾驶汽车的接受度不仅取决于自动驾驶技术本身的可靠性与安全性,而且还将取决于这些数据驱动的智能产品不会导致用户遭遇歧视、操纵、邮件骚扰、不当追踪等权益受侵害之情形。一旦消费者认为自动驾驶汽车危及他们的隐私或自主权,这些智能车辆恐将难逃市场抵制。① 相反,若能充分尊重用户隐私进而赢得他们对自动驾驶汽车的信任,那么自动驾驶汽车市场化的阻力就将大幅减少或从根本上清除。这也表明,隐私保护对确立用户信心乃至对抗不当监控至关重要:首先,用户信任是自动驾驶汽车获得足够市场占有率的重要前提,没有足够的市场支撑,也就难以进一步从安全、效率、交通流量等方面改善自动驾驶技术;其次,由于担心被不当监控,用户使用智能网联平台时就会犹豫不决,这同样会阻碍自动驾驶技术的发展。简言之,自动驾驶汽车对用户隐私的挑战在所难免,如何回应这一挑战关系到消费者能否接受并使用这些智能车辆。同样地,在数据驱动的其他商业场景中,上文所述的隐私危机一样存在。

二、个人控制:数据隐私挑战的立法回应

(一)欧式立法:"权利话语"下的数据保护

在欧洲,"数据隐私被视为基本权利和法律文化的一部分"。② 为此,《欧洲人权公约》第 8 条规定,个人享有"私人和家庭生活被尊重的权利"。除此项传统的隐私权之外,《欧盟基本权利宪章》(以下简称《权利宪章》)第 8 条第 1 款还特别规定"人人有权保护自己的个人数据"。尽管该"个人数据保护权"在表现形态上突破了传统隐私权的特征,但它仍是隐私权在移动互联网条件下的升级形态,正如欧洲法院指出的,两者紧密关联,欧盟委员会在《欧盟一般数据保护条例》(以下简称《条例》)制定过程中也特别强调了这点。③ 成员国层面上,"个人数据保护权"也多被视为基本权利。例如,西班牙、波兰、捷克、希腊、波兰、匈牙利、斯洛伐克等国也都在宪法上或通过司法解释将数据保护权视为一项基本权利。④ 总之,"整个欧洲是在公民基本权利层面上定位个人数据保护的,将对个人数据的保护视为对基本人权的保护"。⑤

由于数据处理可能危及数据主体固有权利,因此《权利宪章》第 8 条不仅规定了个人数据处理应具备明确的法律依据或取得数据主体同意,而且还确立了公平的数据处理、基于特定目的处理数据等法定要求,并授予数据主体访问数据以及更正其个人数据等权利。《条例》第 5 条则从合法性、目的限制、准确性、限期储存、安全性等方面继受并进一步拓展了数据处理的一般原则。总体上,欧洲数据隐私立法遵循"个人数据是人的延伸,人应当独立自主,因而个人数据亦应当由数据主体掌控,体现个人的意志"这一基本逻辑,而"建立在人的尊严基础上的个人数据保护理论,则内含个人数据由个人自主控制的基本论调"。⑥

欧洲数据立法并未忽视信息的自由流动。立法者意识到,保护自然人对其个人数据的控制可能与信息的自由获取及传播存在冲突,因此他们的一贯立场是:数据隐私保护应充分考虑个人数据在社会中的功能,且应与其他人权及基本自由相协调。由此,《欧洲个人数据处理中的个人保护公约》等立

① See Dorothy J. Glancy, Privacy in Autonomous Vehicles, 52 Santa Clara Law Review, 1225 (2012).

② Paul M. Schwartz et al., Transatlantic Data Privacy Law, 106 Georgetown Law Journal,126 (2017).

③ 参见刘泽刚:《欧盟个人数据保护的"后隐私权"变革》,《华东政法大学学报》2018 年第 4 期。

④ See Paul M. Schwartz et al., Transatlantic Data Privacy Law, 106 Georgetown Law Journal, 126 (2017).

⑤ 高富平:《个人信息保护:从个人控制到社会控制》,《法学研究》2018 年第 3 期。

⑥ 高富平:《个人信息保护:从个人控制到社会控制》,《法学研究》2018 年第 3 期。

法只是把个人数据受保护的权利界定为“个人数据保护权”而非“个人数据权”，该权利虽包含了本人对其个人数据及其处理的控制权，但这种控制权不得妨碍信息自由、公众知情等其他基本权利，须在这些基本权利获得充分保障的框架中方能行使。[①]《条例》重申并贯彻了这一立法宗旨。申言之，《条例》虽承认自然人对其个人数据及其处理享有控制利益，但并未承认其为一项独立的法定权利，而是通过赋予自然人一组具体的数据权利，包括数据访问权、更正权、删除权、移转权、拒绝权等，从而保障数据主体了解哪些类型的个人数据被收集以及将被用于何种用途，力图在实现本人对其个人数据的控制从而体现对人的尊重的同时，避免妨碍个人数据的正当使用。此外，为增强对个人数据的保护，欧盟立法者还要求数据控制者建立“隐私设计”和“隐私默认”机制，并在涉及个人数据自动化处理、个人敏感数据处理、或对公共场所进行大规模监控等可能危及个人权利与自由的情形下进行“数据保护影响评估”。

不过，在“权利话语”下，“比信息自由流动更重要的还是维护欧洲权利制度中人的尊严与隐私”。[②]《条例》贯彻了这一价值取向，并强化了数据主体对其个人数据的控制利益以及其主体性地位，如要求数据控制者不得仅仅根据自动化处理而作出对数据主体具有法律或类似重大影响的决策，且不得要求数据主体放弃访问权、更正权等数据权利以换取服务。尤其是，作为一般原则，反映数据主体种族或民族背景、政治倾向、宗教信仰的个人数据、基因数据以及与数据主体健康、性活动有关的数据等均不得处理。总之，由于关乎民主自治且为避免数据主体在数据实践中被视为客体，欧盟隐私立法严格限制可能危及个人隐私权的自动决策，并对数据主体的交易能力或放弃自身权利行为施加限制，要求他们不得通过同意之方式“售卖”受《权利宪章》保护的基本权利。[③]

制度构成上，自动驾驶场景中的隐私问题同样适用欧盟上述关于隐私与数据保护的综合立法。2018 年欧洲议会发布的《合作式智能交通系统欧盟战略报告》强调数据处理应遵守《权利宪章》，并指出自动驾驶汽车产生及传输的数据构成个人数据且应遵守《条例》及相关规则。此外，欧洲议会还于 2017 年 10 月通过了《欧盟电子隐私条例(草案)》(以下简称《草案》)提案，这是欧盟又一项应对物联网时代隐私挑战的立法行动，旨在对《条例》进行补充且将优先适用，其将全面保护隐私权与通信秘密、促进物联网的可信度与安全性，包括自动驾驶中车与车、车与交通基础设施以及个人之间的通信都将受其约束。作为欧洲数据隐私立法的一部分，《草案》进一步强调对私人和家庭生活以及通信的尊重，包括在个人数据处理中对自然人的保护，且充分体现了本人对其个人通信数据的控制。例如，《草案》第 6 条规定，除非用户同意或有其他例外规定，否则不得窃听、存储、监控、扫描或以其他方式拦截、监控或处理用户电子通信数据尤其是位置与交通数据。

(二)美式立法：“市场话语”下的隐私保护

在美国，最初由沃伦和布兰德于《论隐私权》一文构建的隐私侵权理论曾一度被视为隐私保护立法的开创性力量。[④] 该理论后被普罗瑟具体化为侵害他人生活安宁、披露令人尴尬的私人事实、使他人处于为人误解境地、擅自利用他人姓名或其他人格利益等侵权行为，[⑤]并被《美国第二次侵权法重

① 参见高富平：《个人信息保护：从个人控制到社会控制》，《法学研究》2018 年第 3 期。

② See Paul M. Schwartz et al., Transatlantic Data Privacy Law, 106 Georgetown Law Journal, 131 (2017).

③ See Paul M. Schwartz et al., Transatlantic Data Privacy Law, 106 Georgetown Law Journal, 140 (2017).

④ See Benjamin E. Bratman, Brandeis and Warren's "the Right to Privacy and the Birth of the Right to Privacy", 69 Tennessee Law Review, 624 (2002).

⑤ See William L. Prosser, Privacy, 48 California Law Review, 389 (1960).

述》采纳,形成美国早期隐私保护的基本范式。至此,“不受侵扰的权利”或“隐私即秘密”理念开始深入人心。本质上,美国传统隐私保护着眼于将隐私权理解为一项消极的、不被侵害的权利,一定程度上忽视了隐私的社会价值。

随着信息及网络科技的兴起,将隐私视为独处权利或秘密的传统隐私观念被认为无法适应社会经济现实的需要,更无法应对数据时代的挑战。于是,隐私侵权理论的影响渐而式微,“隐私控制论”开始崭露头角并逐渐占据主导地位。①“隐私控制论”强调人们对隐私的支配,即“个人、团体或机构有权自主决定何时、以何种方式以及在多大程度上将其本人信息披露给他人”。② 申言之,“隐私控制论”下的隐私权是指本人对其个人数据使用予以控制的权利。这种自由主义的自治原则力图将本人作为个人数据使用的决策者,借由本人对其个人数据的管理以及本人决定个人数据的使用从而实现“信息自决”。③“隐私控制论”者认为,在法律承认个人数据为财产的情形下,财产法规则能更好地保护个人利益与社会整体利益。因此,他们鼓励人们将“个人数据/隐私视为商品”并倡导通过财产法规则而非侵权规则保护个人数据。④ 正如美国学者劳伦斯·莱斯格所言,在信息时代,“个人必须具有针对隐私进行协商的能力,并享有默认的隐私权。这正是财产概念的意图,那些希望得到财产的人必须在协商成功后才能把它拿走”。⑤

总之,美国理论界普遍认为,个人数据受到保护的根本原因在于它是一种财产。⑥ 正因如此,美国隐私立法以数据自由流动为原则,个人数据的采集、处理及使用以法律明确禁止为限。实践中,美国信息隐私监管主要依赖行业自律以及联邦贸易委员会事后执法对“不公平或欺骗性”数据行为进行查处。相比之下,欧洲关于隐私保护秉持一贯的人权立场:因为隐私关涉人格且关乎每个人的个体完整性,所以隐私不可商品化。⑦ 换言之,在“权利话语”下,数据隐私属欧盟公民的基本权利与自由范畴。因此,欧盟隐私及数据保护立法对于数据收集、使用以及公开更具限制性,包括严格的知情同意要求。较之于欧盟,美国法律并未明确要求数据处理应具有个人“同意”等法律依据,而是要求数据控制者就其数据处理的隐私政策进行“告知”并由隐私消费者自行决定“留下”还是“离开”。⑧ 这意味着数据控制者若就其隐私政策进行告知,那么消费者随后分享其个人数据的行为将被视为同意。此即美国式“知情—选择(同意)”隐私自治机制——经由知情、访问以及同意等与个人数据采集、使用以及公开相关的一系列权利,隐私消费者获得了对其个人数据的控制权。据此,他们可以自行衡量关于其个人数据的采集、使用或公开的成本与收益。⑨ 实践中,“知情—选择(同意)”机制不仅被美国隐私执法机构引入与自动驾驶汽车有关的政策框架之中,而且还在自动驾驶汽车隐私保护最新立法议案——美国参议院提出的《汽车安全与隐私法案》以及众议院审议通过的《自动驾驶法案》——中得到

① See Daniel J. Solove, Understanding Privacy, Harvard University Press, 2008, p.24.

② Alan F. Westin, Privacy and Freedom, Atheneum, 1967, p.7.

③ See Paul M. Schwartz, Internet Privacy and the State, 32 Connecticut Law Review, 820 (1999—2000).

④ See Paul M. Schwartz, Internet Privacy and the State, 32 Connecticut Law Review, 820 (1999—2000).

⑤ [美]劳伦斯·莱斯格:《代码:塑造网络空间的法律》,李旭等译,中信出版社 2004 年版,第 197 页。

⑥ 参见程啸:《论大数据时代的个人数据权利》,《中国社会科学》2018 年第 3 期。

⑦ See Corien Prins, Property and Privacy: European Perspectives and the Commodification of Our Identity, 16 Information Law Series, 223—257(2006).

⑧ See Paul M. Schwartz et al., Transatlantic Data Privacy Law, 106 Georgetown Law Journal, 152—155 (2017).

⑨ See Daniel J. Solove, Introduction: Privacy Self—management and the Consent Dilemma, 126 Harvard Law Review, 1880 (2013).

了贯彻。

基于各自传统，欧美立法者针对数据驱动商业场景尤其是自动驾驶隐私挑战作出了初步的立法回应。总体而言，美国缺乏类似于欧洲数据保护法中的“个人数据保护权”，相反，借用侵权法或财产规则保护隐私才是典型的美国实用主义处理问题的方式，凸显了欧美在隐私保护上的理论分野：欧洲围绕“权利话语”创建隐私文化，数据隐私被视为人的基本权利范畴，关乎人的尊严；美国则着眼于“市场话语”，将隐私视作一种应受保护的市场利益，个人被视为应免受市场欺诈和不公平对待的隐私消费者。① 这种价值上的分歧很大程度上源于欧美国家不同的社会、政治和法律传统：在美国的政治话语中，人们多是担心国家而非私人公司侵犯个人隐私，且市场被视为是隐私保护的最佳工具；相反，在欧洲的政治话语中，自由资本主义被认为是隐私受到侵犯的罪魁祸首，因此人们更多担心私人公司尤其是那些大数据公司对个人隐私的侵犯，于是公众指望数据保护机构发布相应的指南或有约束力的法规以保护他们的隐私选择。② 所有这些对欧美包括自动驾驶场景在内的隐私/数据保护立法产生了深远影响。不过，值得注意的是：一方面，虽然欧美在隐私立法价值取向上截然不同，但在制度层面，两者又不约而同地强调本人对其个人数据/隐私的控制，要求个人数据使用满足目的合法、数据最少化、用户知情等限制性要求，维护数据主体的尊严或自由不因个人数据滥用而遭受侵害；另一方面，为避免妨碍信息自由流动尤其是数据产业的发展，无论是欧洲国家还是美国，均未将本人对其个人数据的控制利益上升为排他性的个人法定权利或将隐私/个人数据客体化为个人绝对支配的对象。

（三）中国立法中的个人控制：兼与欧美比较

学理上，国内学者有从私人生活安宁与生活秘密视角定义隐私权，③亦有从控制视角阐释隐私权。④ 这些定义试图在私人领域与公共领域两个对立的二元空间划分中探寻隐私权的本质，存在要么过宽、要么过窄的问题。虽然“似乎无人知道隐私为何物”⑤之论断过于悲观，但隐私权极难定义确是不争的事实。事实上，“隐私权的范围是一个动态平衡的范围”。⑥ 因此，与其陷入概念纷争，不如从实用主义出发，把隐私权看成是“开放的体系”，一个个不同而又相似的隐私将因此形成“一个隐私系列”。⑦ 如今，大数据已可量化一切，消费者的期望、观点、心理、行踪、消费习惯等都可被“数据化”。数据控制者可据此从事相关性分析，进行预测或推断而非因果关系解释。而且，移动互联网技术已使网络空间与现实世界乃至私人与公共领域的边界变得越来越模糊，越来越多的人乐于分享自己的个人活动、生活场景甚或思想观点。因此，开放的隐私观或许才是呼应大数据时代隐私挑战的合适选择。如此，至少可把数据控制者通过相关性分析从而预测或推断出的某种“事实”（“预测性隐私”）纳入隐私权保护范围。

立法上，继《中华人民共和国侵权责任法》第2条明定隐私权之后，《中华人民共和国民法总则》

---

① See Paul M. Schwartz et al., Transatlantic Data Privacy Law, 106 Georgetown Law Journal, 119 (2017).

② See Pierluigi Perri et al., Ancient Worries and Modern Fears: Different Roots and Common Effects of U.S. and E.U. Privacy Regulation, 49 Connecticut Law Review, 1625－1624 (2017).

③ 参见王利明：《隐私权概念的再界定》，《法学家》2012年第1期。

④ 参见杨立新：《人格权法》，法律出版社2011年版，第599页。

⑤ See James Q. Whitman, The two Western Cultures of Privacy: Dignity Versus Liberty, 113 Yale Law Journal, 1153 (2004).

⑥ 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。

⑦ 转引自王立志：《隐私权之定义是否可能》，《政治与法律》2015年第8期。

(以下简称《民法总则》)第 110 条再次确认了自然人享有隐私权这项独立的人格权利。2019 年 12 月公布的《中华人民共和国民法典草案(三审稿)》[以下简称《民法典草案(三审稿)》]第 1032～1033 条关于隐私的立法仍遵循传统的隐私侵权理论,即将隐私权视为一项消极的、不被侵扰的权利,但作为缓和,又通过"权利人同意"赋权个人自行决定自己的隐私命运,尊重个人对其隐私的积极利用而非一味地消极防御。此外,由于《民法总则》第 111 条另行规定"自然人的个人信息受法律保护",因此引发了个人信息到底是法益还是独立民事权利的理论争议,并衍生出隐私权与"个人信息权"界分问题。比较法上,美国并无隐私与个人信息保护的二分法,而是采"信息隐私"之概念并演绎出市场主义的"隐私控制论";欧盟则在传统隐私权之外,另定个人数据保护规范,经由"个人数据保护权"化解数据隐私与数据利用之间的内在冲突。鉴于"一条条个人信息的价钱少得可怜,除非被收集的数据与更多来自相近社会经济类别的个人数据予以整合并加以利用,否则这些数据将一文不值",[①]因此若承认自然人对个人数据享有权利,那么将其建立在维护人格尊严与自由而非所谓财产自由基础之上则更具说服力,这也正是欧盟数据隐私保护的根本出发点。我国司法实践中也多是审查收集、使用个人信息的行为是否侵犯了自然人的隐私权、名誉权或其他一般人格权。

值得注意的是,我国个人信息保护立法同样强调个人控制,且较之于欧美有过之而无不及。2012 年《关于加强网络信息保护的决定》第 2 条首次规定收集、使用个人信息应经被收集者"同意"后,《中华人民共和国网络安全法》第 22 条和第 41 条、《征信业管理条例》第 14 条第 2 款等随即继受了用户"同意"这一收集、使用个人信息的前置性要求,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》第 12 条第 1 款亦明确将"同意"作为网络用户或网络服务提供商公开他人隐私或其他个人信息免于承担侵权责任的豁免理由。《民法总则》第 111 条关于获取他人个人信息"应当依法取得"之规定亦不难解释出个人"同意"的意涵。《民法典草案(三审稿)》第 1034～1038 条则吸纳了现有个人信息保护的基本原则与制度内容,并增加了自然人对其个人数据的查阅权、更正权以及删除权等数据权利。这些规定与欧美隐私立法中的个人控制导向并无本质差异,均反映了立法者对数据主体尊严或自由的尊重。不过,相较于我国个人信息保护立法将"同意一般化",[②]欧盟仅将"同意"作为个人数据收集、处理及使用的法律依据之一,而非唯一的合法性基础,如为订立和履行合同,数据处理行为即无须用户"同意";美国法则只是强调场景不一致情形下的数据处理及利用行为需获得用户"同意"。无论如何,正如欧美隐私立法所表明的,"个人控制"仅仅是维护数据实践中个人自治的手段,旨在保护本人在其个人数据被采集、处理等过程中的自我决定或控制性利益,而非借此将本人对其个人数据的控制推演为"个人数据权"这一绝对的法律权利。只不过,随着个人数据逐渐由数据主体转为具有垄断性数据处理能力的数据控制者掌控,"个人控制"的实际效果并不如预期。

三、"控制"的错觉:现有数据隐私立法取向的审视

不难看出,个人控制原则的基本假设是:将数据主体视为理性且自主的角色,推定他们有能力对收集、处理及利用其个人数据的行为进行损益评估,并能对数据控制者是否根据其同意的目的或方式

① See Joseph W. Jerome, Buying and Selling Privacy: Big Data's Different Burdens and Benefits, 66 Stanford aw Review Online, 52 (2013).

② 高富平《个人信息保护:从个人控制到社会控制》,《法学研究》2018 年第 3 期。

使用个人数据之行为进行监督或控制。然而，现有强调个人控制的程序主义隐私保护策略很大程度上就是“一个错觉”。[①] 产生这一“错觉”的原因在于过于相信或依赖个人的自治能力，建立在这一理论假设之上的隐私保护框架难以确保数据主体对其个人数据进行有意义的“控制”。

一方面，基于个人控制的隐私保护策略面临数据主体有限理性或认知能力不足的挑战。行为经济学观点——个人在隐私保护方面的非理性行为——已经得到了广泛的证据支持，[②]包括人们很少甚或完全忽视通过阅读隐私条款、清除上网记录、关闭智能设备位置追踪功能等方式保护自己的隐私。实际上，为享受更便利的数字产品或服务体验，人们多半会选择披露自己的个人数据，而非以所谓“理性人”的审慎态度寻求最低限度地公开甚至完全拒绝公开自己的个人数据。[③] 这意味着，在数据实践中，立法者所假定的“理性人”的一些“非理性行为”势必损及其在事关收集、处理及利用其个人数据的决策中作出理性选择的能力。当然，人们忽视或主动放弃仔细阅读隐私政策多少有点迫不得已：(1)研读冗长的隐私政策耗时费力，消费者因此需要承担高昂的机会成本，包括比较相近产品或服务提供者制定的隐私政策或声明所耗费的额外成本；[④](2)令人迷惑的技术以及法律上的繁文缛节致使隐私政策或声明变得晦涩难懂或模糊不清。

另一方面，即便是明智且理性的个人恐怕也将因一些结构性问题而无法适当管理自己隐私，特别是机器学习等复杂“算法”正在被不断地用于数据的收集与处理，消费者对其个人数据用于社会及商业网络的行为进行监督或控制变得越来越困难。(1)复杂的“算法”正使我们的社会日益成为“黑箱社会”，而“解构大数据这一黑箱是如此不易，就算数据掌控者愿意披露他们的‘算法’，现代互联网也为理解它们设置了巨大障碍”。[⑤] (2)鉴于彼此关联的数据企业实在太多，加之物联网已使数据共享、复制与转移变得极为便捷，以至于许多情形下的隐私损害往往是不同业者掌握的数据融合后导致的结果，而且在多数情形下，数据收集者的隐私政策对于共享或受让数据的“关联方”或“第三方”的说明往往模糊不清，因此在不了解个人数据后续用途或将被谁占有使用的情形下，要求数据主体进行所谓的损益评估几乎是不可能的，如此一来，隐私自我管理的成效自然要打折扣。[⑥] 进言之，即使本人有能力进行损益评估，但鉴于隐私的成本与收益还需从整体而非个人层面进行评估，因此由个人决定是否同意数据的采集、使用或公开很难产生最佳的社会效果，[⑦]甚至将导致每个人获得的数据福利被大幅削减或消失。(3)如果消费者获得数字产品或网络服务是以其放弃个人数据为条件，而且也没有可替

① See Neil M. Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law, 19 Stanford Technology Law Review, 444 (2016).

② See Alessandro Acquisti et al., Privacy and Human Behavior in the Age of Information, 347 Science, 509 (2015).

③ See John A. Rothchild, Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online, 66 Cleveland State Law Review, 614 (2018).

④ See John A. Rothchild, Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online, 66 Cleveland State Law Review, 615－616 (2018).

⑤ Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information, Cambridge, Harvard University Press, 2015, p.6.

⑥ See Daniel J. Solove, Introduction: Privacy Self－management and the Consent Dilemma, 126 Harvard Law Review, 1881 (2013).

⑦ See Daniel J. Solove, Introduction: Privacy Self－management and the Consent Dilemma, 126 Harvard Law Review, 1881 (2013).

代的相近产品或服务的话,那么所谓的“选择”恐怕就徒具形式了。①

具体到自动驾驶汽车,程序主义范式的数据隐私保护暴露出来的问题更突出。相对于动态的自动驾驶场景,“知情—选择(同意)”机制过于静态且程序繁琐,智能交通中的数据控制者面临难以取得用户同意这一现实困难:现有立法中关于知情同意的规定,不仅意味着数据主体应积极明确地对数据收集与使用行为表明态度,而且还需要他们知晓请求同意的主体、被收集的数据的类型以及数据处理的目的。然而,在自动驾驶场景中,这一法律要求将遭遇挑战:(1)自动驾驶要求数据交换即时发生甚至是随机发生,因此获得用户“同意”即便可能,那也极端困难;(2)鉴于自动驾驶汽车安全性能依赖于实时且不间断的数据交换,因此完全由个人凭自己意愿作出“真正的选择”几乎是不可能的,任何要求中断连接以获得用户经过深思熟虑而后作出“同意”或“选择”都可能危及交通安全。②

综上所述,隐私保护的个人控制取向确有不足之处。正因如此,激进观点认为,不应再将“同意”作为个人数据处理的正当基础;③还有观点强调个人数据的公共属性,甚至以维护公共利益以及促进个人数据自由流动为名,否定本人对其个人数据的民事权利并将个人数据作为公共物品从而通过公法规制。④ 然而,最新立法表明,“个人控制”仍是隐私保护与个人数据监管的基本范式。例如,印度联邦内阁 2019 年底提交国会审议的《个人数据保护法案》就确认数据共享中个人“同意”的神圣性。笔者认为,“个人控制”是对数据主体自治、自决与主体性的体现,贬低甚或抛弃这一原则恐将“削弱个人参与他人管理个人数据时的权利和能力”。⑤ 当然,我们也不讳言“个人控制”的理论假设低估了大数据对个人自治能力的挑战。但无论如何,“不完美的自主总比没有机会自主好,认为个人行使不好权利就不赋予其权利的逻辑显然存在严重问题”!⑥ 况且,数据主体对其个人数据的自主控制并不必然与个人数据的合理利用形成不可调和的紧张对立关系。事实上,立法者已在制度上设置了诸多例外情形进而缓和了“个人控制”对数据利用的制约。总之,“个人控制”取向的隐私保护策略仍具显著价值。只是,在未来的数据隐私保护优化方案中,还应考虑把焦点从数据主体的隐私自治扩展至数据控制者的自我约束,构建能增强后者问责性的理论框架,填补现有隐私管理中的“自治陷阱”。

四、数据信义义务:数据驱动时代隐私保护的优化

不得不承认,大数据企业在现代经济与社会生活中正发挥着难以替代的作用,它们不是在反映而是在塑造某种社会规范。⑦ 借助难为常人所理解的算法,数据控制者已变得越来越有权力,而数据主体已沦为数据关系中的弱者,他们对个人数据的自主控制权正日益减损以至于变得越发依赖数据控

① See John A. Rothchild, Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online, 66 Cleveland State Law Review, 613 (2018).

② See Ivan L. Sucharski et al., Privacy in the Age of Autonomous Vehicles, 73 Washington and Lee Law Review Online, 735—736 (2017).

③ 参见任龙龙:《论同意不是个人信息处理的正当性基础》,《政治与法律》2016 年第 1 期。

④ 参见吴伟光:《大数据技术下个人数据信息私权保护论批判》,《政治与法律》2016 年第 7 期。

⑤ Serge Gutwirth et al., Reforming European Data Protection Law, Dordrecht: Springer, 2015, pp.296—297.

⑥ 田野:《大数据时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例》,《法制与社会发展》2018 年第 6 期。

⑦ See Jeffrey Rosen, the Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google, 80 Fordham Law Review, 1535 (2012).

制者。数据控制者与数据主体之间显著的知识与信息不对称，包括对个人数据控制力的强弱之分，加之数据主体对公开个人数据的实际影响缺乏必要了解，从而导致他们在保护自己隐私时面临严峻挑战。毕竟，大数据分析对于普通用户而言就像一个“黑洞”，他们既不了解数据的存储，也不知道数据企业利用这些数据创造价值的方式，有时连数据分析者自己恐怕都无法预见能否从其聚集的数据中获得有什么价值的东西。①

鉴于隐私管理中的“自治陷阱”，尤其是数据控制者在权力、信息等方面享有的不对称优势，不防换个角度，从信赖视角理解隐私或数据关系并为数据控制者制定更高的行为标准。其实，“隐私并非排他性地与个人选择、自治或隐居概念捆绑在一起，相反，它是一种基于个人与个人以及个人与机构之间信任关系的社会事实……我们因信任而共享信息并在此背景下保留隐私权……对隐私的合理期待就是对信任的期待”。② 可以肯定地说，“信任无处不在……我们相信设计师与建造者完成的桥梁足以确保我们安全通行……相信飞机将安全飞行并达到正确的目的地，相信专业人士在提供服务时以我们的最佳利益为重……总之，没有信任，现代政府、商业和社会制度本身都将崩溃”。③ 数据时代更不例外。一旦把隐私概念化为信任或信赖，就会发现它对商业的重要性：一方面，数据控制者每次要求消费者提供个人数据时须借助这种信任；另一方面，若它们过度利用用户信任，或者用户一旦认为与数据控制者共享个人数据将有损自身利益，那么他们势必会大幅减少与其共享的信息量或干脆拒绝共享其个人数据，这意味着数据产业赖以生存的基础——数字信任——行将崩溃，最终将损及数据控制者自身。④

一般认为，如果一方因另一方的才识从而信任并依赖他，那么两者之间就可构成信义关系。⑤ 具体而言，当我们访问网站、搜索查询、网上购物以及提供个人数据时，多半是因为相信这些交易相对方在提供数字产品与服务时会保护好我们的个人数据，更不会滥用这些数据。这是一种“特殊的信任——数字信任，它蕴含着我们对数字产品与服务提供商利用个人数据是使我们受益而非损害我们利益的基本信念”。⑥ 这无异于资产管理人等传统专业人士与其客户之间基于信任而形成的特殊关系，均可视为信义关系。它们的共同点在于：信息不对称且双方都明了弱势一方信任或依赖占据信息优势的一方。⑦ 因此，可将数据控制者视为数据受托人，它们因与数据主体之间的服务关系从而获取并控制这些消费者的个人数据，为避免数据控制者利用其不对称优势因而应要求他们负担特定义务；

---

① See Dennis D. Hirsch, Privacy, Public Goods, and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel, 65 Duke Law Review Online, 75－76 (2016).

② Ari Ezra Waldman, Privacy as Trust: Sharing Personal Information in a Networked World, 69 University of Miami Law Review, 561 (2015).

③ Neil M. Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law, 19 Stanford Technology Law Review, 433 (2016).

④ See Dennis D. Hirsch, Privacy, Public Goods, and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel, 65 Duke Law Review Online, 83 (2016).

⑤ See Robert A. Kutcher, Breach of Fiduciary Duties, in David A. Soley et al., Business Torts Litigation, American Bar Association, 2005, p.3.

⑥ Dennis D. Hirsch, Privacy, Public Goods, and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel, 65 Duke Law Review Online, 83 (2016).

⑦ See Ariel Dobkin, Information Fiduciaries in Practice: Data Privacy and User Expectations, 33 Berkeley Technology Law Journal, 10 (2018).

相应地,将个人数据“托付”给数据控制者的数据主体则成为委托人。① 笔者认为,数据受托人概念的引入有助于重新定位隐私并将信义义务嵌入新型的数据关系之中,促使数据控制者成为一个值得信赖的角色,并“确保大数据应用不至于导致个人隐私的终结”。② 更重要的是,在基于信任的隐私保护框架下,违背信任的行为本身即可被视为可诉行为,很大程度上,损害的量化或证明问题将因此而迎刃而解。③

本质上,将信义义务或其要素引入新型数据关系之中,并非取代而是充实现有基于个人控制的隐私保护框架,旨在要求数据控制者以数据受托人身份参与数据实践,从而使其负担更高的义务标准并据此增强它们的问责制。其基本理念是,要求数据关系中的强者——那些具有数据垄断地位的数据控制者——负担更高标准的义务,不再仅仅依赖弱势的甚或正在丧失自主控制权的数据主体的隐私自治。进一步而言,以谨慎、保护与忠实等实质性义务重塑秘密、安全及透明度等传统的隐私概念,数据控制者应把数据主体利益置于它们自己的短期利益之上,在收集、使用或共享个人数据时有责任避免不合理且危险的自我交易或其他有害行为。④

申言之,首先应引入谨慎要求。该要求旨在促使数据控制者在数据实践中谨慎行事,它们既不得以“侵犯信息主体的利益或者违反信息主体的合理预期的方式使用和披露个人信息”,而且也“有义务确保个人信息的下游使用是合理的、合法的”。⑤ 虽然大多数国家的隐私法将保密概念化为不公开义务,但事实上人们公开自己个人数据时所持的最基本假设是数据控制者是谨慎行事之人,因此数据控制者若能谨慎从事数据收集、处理或利用等行为,包括获取个人同意并遵从合法性、目的限制、数据最小化与准确性、限制存储以及数据处理透明等基本原则,人们就会相信它们并愿意参与那些需要使用个人数据的商业与社会活动,这不仅能惠及个人,整个社会也将受益;而且,违反保密义务的侵权行为责任也将因谨慎要求的引入而得到增强。⑥

其次,数据控制者应以受托人身份保护其占有的个人数据。“保护义务”的要求旨在将隐私保护理念嵌入更广的数据安全管理体系中、致力于隐私保护而非仅仅是避免被黑客攻击或其他形式的非法访问等传统的数据安全管理。⑦ 以数据“保护义务”替换“安全保障义务”不仅不是废弃后者所强调的采取必要措施防止数据泄露这一关乎“数据安全”的关键举措,而且还将在更广泛的范围内要求数据控制者提高数据安全保障水平,侧重点不再是数据控制者是否采取了安全保障措施而是其采取的措施是否符合行业的普遍标准甚或是用户的合理期待。这些安全保障措施不仅应与数据受托人处理

---

① See Neil M. Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law, 19 Stanford Technology Law Review, 449－450 (2016).

② See Ariel Dobkin, Information Fiduciaries in Practice: Data Privacy and User Expectations, 33 Berkeley Technology Law Journal, 49 (2018).

③ See Neil M. Richards & Woodrow Hartzog, Privacy's Trust Gap: A Review, 126 Yale Law Journal, 1216 (2017).

④ See Neil M. Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law, 19 Stanford Technology Law Review, 450－457 (2016).

⑤ 吴泓:《信赖理念下的个人信息使用与保护》,《华东政法大学学报》2018 年第 1 期。

⑥ See Neil M. Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law, 19 Stanford Technology Law Review, 459－462 (2016).

⑦ See Neil M. Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law, 19 Stanford Technology Law Review, 465－468 (2016).

的个人数据的性质、范围和目的、与该数据处理行为有关的风险以及该处理行为致害的可能性或严重性相一致，而且还应根据法定或行业规定方式定期审查并进行相应升级或适当调整。当然，诸如匿名化和加密处理、去中心化存储等事关数据安全的要求、数据泄露后的通知（报告）义务以及采取补救措施这一止损义务自然就成为数据控制者履行保护义务的应有之义。

最后，数据控制者尤应遵守忠实义务要求。“知情－选择（同意）”程序设计虽在一定程度上能确保数据收集、使用与公开等行为保持透明，但事实上，数据控制者几乎不会关心数据主体是否了解告知内容的真正含义。同时，也无法指望用户自己认真阅读那些艰难晦涩的隐私条款。鉴此，以忠实义务标准取代透明度要求，能有效促使数据控制者以更积极的措施确保数据主体真正理解数据处理行为对其自身的影响，因为较之于充满枯燥说辞或模糊保证的隐私政策声明，信任机制更直观、更有效用。① 如此一来，数据控制者实施的操纵（仅仅试图改变另一方行为的情形并不构成操纵，意图规避他人“深思熟虑的能力”、导致一方当事人并非基于自己自由意志作出决定的行为才是）、歧视（个人权利或某种机会因数据“画像”而丧失或因此承担其他人无须负担的额外成本等数据滥用行为，如数据控制者为其认定的“高价值”客户提供更高价格商品的行为，以及利用数据相关性分析从而预测某人未来罹患严重疾病的风险进而拒绝向其提供工作机会或保险服务等情形）、未经用户授权或超过其授权使用、违背自身隐私政策等短期逐利行为都将构成对忠实义务的违反。毕竟，这些数据滥用行为都与用户“合理期待”背道而驰。② 正所谓，“如果你劝诱他人相信你，你就不能转身背叛他的信任”。③

进一步而言，《民法总则》第7条关于诚信原则的规定已然构成信任责任法的基础。因为，在内涵上，这一规定与英美法上的信义法所强调的忠诚地对待信任、诚实履行义务、遵守合理的商业标准、不得欺诈或获取不当利益等基本法理是相通的。④ 值得注意的是，我国杭州等地互联网法院的设立为涉及个人数据及网上隐私保护等民事纠纷的解决提供了先行先试的机会与组织保障。⑤ 尤其是，法院可考虑通过对诚信原则的灵活性解释，阐明其中所蕴含的信义法理，并以样本案例为指导，逐步确立数据受托责任判定标准。首先，对数据控制者或网络服务提供商进行定义以明确承担数据受托责任的主体类别或范围，尤其是像百度、阿里、腾讯等大型数据公司或社交媒体中介因用户信赖程度更高从而可能负担比其他普通或不知名的网络服务提供商更高标准的信义义务。⑥ 其次，确定“理性用户”的期望该是什么或对“理性用户”进行“画像”。毕竟，数据受托责任建基于用户的“合理期待”。当用户将其个人数据“托付”给数据控制者时，也就一并将对后者的信任与依赖嵌入了数据关系之中，且选择相信数据控制者会尊重并保护他们的数据隐私，任何利用数据“画像”不当改变其选择或决定甚

① See Neil M. Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law, 19 Stanford Technology Law Review, 462－465 (2016).

② See Ariel Dobkin, Information Fiduciaries in Practice: Data Privacy and User Expectations, 33 Berkeley Technology Law Journal, 18－47(2018).

③ Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 UC Davis Law Review, 1224 (2016).

④ 参见赵磊：《信托受托人的角色定位及其制度实现》，《中国法学》2013年第4期。

⑤ 参见高薇：《互联网争议解决中的执行问题——从司法、私人到去中心化数字执行》，《法商研究》2018年第6期。

⑥ 《印度个人数据保护法案》第26条就引入“重要数据受托人”这一概念，并根据所处理的个人数据的数量、敏感度、数据受托人的营业额及采用的新技术以及数据处理行为的风险等因素予以识别。根据《印度个人数据保护法案》第26～28条的规定，一旦被认定为“重要数据受托人”，其将负担进行数据保护评估、定期进行安全保护措施审查、数据处理政策和行为审计、设立数据保护专职人员等加重义务。这些规定对拟于2020年进行的我国个人数据保护立法具有显著的借鉴意义。

至是歧视他们,都将违背用户的信任或"合理期待"。事实上,正是一方对另一方"合理期待"所塑造的信任和忠实之价值才构成了英美法中信义标准的基础。这种开放式的标准不仅易于适应不断变化的社会需求,而且也有助于促使受托人谨慎地并以更高的标准行事。① 最后,在责任承担上,除停止侵害等传统救济外,还可考虑引入惩罚性损害赔偿,以期给予数据滥用行为足够威慑。不过,自动驾驶以及数据驱动的其他商业场景中的数据控制者之数据受托人的定位与资产管理人等传统受托人仍存在显著的差异:"前者负担的义务范围狭窄,后者则承担相当广泛且强有力的受托责任,很多时候我们期待上述专业人士不仅能主动避免损害客户利益,而且还能关注客户利益并防止他们损害自己或做其他傻事,但无论如何,我们不该对数据企业提出如此苛刻的要求,虽然它们也有保护用户隐私的义务,但不能期待或要求它们对我们某次出行提出警示或阻止用户在社交媒体上披露更多的个人信息"。②

五、结语

个人数据的收集、处理及利用已不可避免地成为社会、经济体系的一部分。作为隐私载体的个人数据已成为一种重要的社会资源,具有显著的社会价值。因此,为促进数据产业发展乃至社会进步,应摆脱数据独占理念进而让更多当事人有机会获取并使用数据。若因隐私保护之故而赋予数据主体对个人数据或隐私的绝对控制,那么就可能阻碍数据产业的发展乃至社会进步。当然,这也绝非意味隐私的消亡。相反,隐私"关乎人们的身份、平等、安全以及信任的建立……只是,大数据时代的隐私不应再被纯粹地当作一种秘密,而是一种处于秘密与完全公开的中间状态,在此意义上说,隐私权不是一种绝对的权利,而是一种相对的权利"。③

鉴于个人数据采集、处理及利用已成为社会及经济生活一部分且很多时候会以牺牲数据主体利益为代价,因此在推动数据产业发展的同时,还应妥善保护用户数据隐私,否则这些消费者将会拒绝使用数据驱动的产品或服务从而主动化解自己遭遇的隐私危机。尽管"隐私已死?"的质问让不少人对即将到来的"透明社会"感到恐惧,但这纯属多虑。不可否认,现有隐私保护存在上文所述的保护不周问题。因此,可创设多维度的隐私保护规则,并将隐私的关注点从保护隐私不受不法或不当行为侵害扩展到将其视为信任关系的推动者,在促进个人隐私自治同时,增强数据控制者问责制,要求它们以数据受托人之身份收集、处理及使用个人数据。总之,在一个技术不断发展的社会中如何对隐私进行定义是隐私保护中最棘手的问题之一,而如何在更广泛的公共利益背景下权衡隐私价值或将是更大挑战。④

责任编辑 何 艳

① See Edward J. Waitzer et al., The Public Fiduciary: Emerging Themes in Canadian Fiduciary Law for Pension Trustees, 91 Canadian Bar Review, 177 (2012).

② Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 UC. Davis Law Review, 1225－1229 (2016).

③ 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。

④ See Robert van den Hoven van Genderen, Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics, 3 European Data Protection Law Review, 339 (2017).