隐私权过时了吗
——数字社会隐私保护的困境与应对

黄 琪

(四川大学 文学与新闻学院,四川 成都 610064)

摘要:隐私权乃维系人类文明之基石,然而数字时代的科技革命全面打破了隐私权功能赖以发挥的传统社会场景与制度规范,深刻瓦解了隐私权的功效,致使隐私保护问题在数字社会成为全球性的公共问题。面对愈演愈烈的隐私危机以及基本失效的隐私权,欧盟与美国分别另行建构风格迥异的个人数据/信息保护体系,将其作为隐私保护的先导机制。我国采取与欧美类似路径,淡化隐私权的作用,另辟个人信息保护制度承接数字社会隐私保护的重任,虽有巨大的时代进步性,但仍需重点关注现存的法律体系结构混乱、碎片化立法等问题。

关键词:隐私;隐私权;数字社会;个人信息保护

[中图分类号]D923 [文献标识码]A [文章编号]1672-934X(2022)02-0104-11

DOI:10.16573/j.cnki.1672-934x.2022.02.014

Is the Right to Privacy Obsolete? The Dilemmas and Countermeasures of Privacy Protection in Digital Society

Huang Qi

(*School of Literature and Journalism, Sichuan University, Chengdu, Sichuan* 610064, *China*)

Abstract: The right to privacy is the cornerstone to maintain human civilization. However, technology revolution in digital era has completely broken the traditional social scene and institutional norms on which the function of the right to privacy depends, deeply disrupted the effect of the right to privacy, and led the issue of privacy protection to becoming a global public issue in digital society. In the face of a growingly fierce privacy crisis and the almost disabled privacy right, the European Union and the United States have respectively constructed different personal data information protection systems as the forerunner mechanism for privacy protection. China adopts a similar path to Europe and America to downplay the role of the right to privacy and create a personal information protection system to shoulder the heavy responsibility of privacy protection in the digital society. Although making great era progress, it still needs to focus on the issues such as the confusion of the legal system structure and the fragmentation of legislation.

Key words: privacy; privacy right; digital society; personal information protection

隐私意识的觉醒及隐私权的发展与人类社会的文明进程息息相关。进入信息时代前,隐私保护问题在很长一段时期内存在感低、关注度弱。从世界范围来看,与其他古老的诸如物权、债权等法律权利相比,隐私权迟至近代资本主义文明阶段才在学理层面出现,正式成为法

收稿日期:2021-11-16

作者简介:黄 琪(1992—),男,博士研究生,研究方向为个人信息保护与媒介法规。

律制度距今也才百来年历史。然而,随着以互联网、大数据、人工智能为代表的新一代信息技术的迅猛发展,大规模的隐私泄露问题开始出现并愈演愈烈。质言之,隐私危机的公共化或普遍化与现代信息社会的进阶具有密不可分的关系。数字社会各种智能科技的快速发展与广泛应用,使公共部门、商业机构等能够方便快捷地搜集、储存、传播有关个人的各种信息,通过不同方式加以组合或呈现,以预测个人的行为模式、政治倾向、消费习惯等,进而作为一种资源或商品加以利用。被侵害者通常难以知悉或防范其信息隐私被窥探、搜集或使用,个人逐渐成为所谓的"透明人"。旧有的行为习惯与制度规范在数字社会遭受极大冲击,引发"个人隐私权终结"之类的群体性恐慌,不仅对社会公共秩序造成严重影响,也给数字经济的创新发展带来一定程度的干扰。尽管隐私权是人本主义在现代文明社会的再现与扩张,乃人之一项不可或缺的基本权利,具有特殊的功能价值,但是数字社会深刻改变了隐私权的运行环境与运行逻辑,无论是作用力还是作用场域,隐私权逐渐式微,致使隐私保护豁口渐有决堤风险。面对这一新变局,究竟是进行隐私权的内部革命还是另辟路径,成为摆在当今国际社会主流法律体系面前不得不抉择的问题。

一、价值辨析:隐私权何以重要

伴随着原始集体生存方式的消亡以及私有制的出现,隐私意识开始觉醒,并进一步产生自我隐私保护的权利。"隐私权"作为一种法律概念,一般认为源自美国学者沃伦(Samuel Warren)和布兰代斯(Louis Brandeis)于 1890 年在《哈佛法律评论》上发表的《论隐私权》一文。当时美国黄色新闻猖狂,新闻报道为了迎合低级趣味,不厌其烦地制造流言,侵犯私人和家庭等领域。针对这一乱象,该文作者认为应当认可普通法上"不受干扰以及独处的权利"。1905 年,在美国"派维斯奇诉新英格兰人寿保险公司"(Pavesich v. New England Life Ins. Co.)一案中,隐私权首次在判例上被承认而正式成为法律权利,并经后续学者的努力不断得到优化。随着全球民主化的进程,隐私权成为一项普适性基本权利。

隐私权是确保个人人格权利完整的关键,其核心要旨在于个人私域之自主权利,保护范围包括个人的生活私密领域与信息自主(信息隐私),其价值本质为人之尊严及自由不受外界操控或支配。在具体化的新兴个别人格权中,以隐私权最为重要,已发展成为一个具有概括性的权利[1](P31)。除上述核心价值功能外,隐私权还具有其他作用,包括民主社会的维持、个人的社会参与、对国家权力的限制等,这些工具性功能的发挥依赖于核心价值的存续。此外,隐私作为一种直达个人内核的封闭性信息,具有巨大的商业财产价值与公共管理价值,为各方所觊觎。隐私权具有强烈的对世性,是确保私人领域自主、对抗外力干预的"保护壳"。任何对此"壳"的破坏,都将构成对自我存在的严重危害,使个人暴露于外,或遭受他人嘲笑、羞辱,或受制于知悉其私密之人。可以说,个人如果被监视、窃听或干涉,将无法对自己的事物保有最终决定的权利,也就不再是自己的主宰,因而会丧失其作为独立个体的地位。在 2016 年的美国总统大选中,剑桥分析公司(Cambridge Analytic)利用 Facebook 泄露的用户信息帮助特朗普量身定制并精准投放竞选广告,为其最终当选总统作出了重要贡献。投票给哪位总统候选人看似是由选民自主选择,实则是通过掌握、洞察选民的信息隐私从而对其投票倾向进行潜移默化的影响与操控,最终导致选民在毫无觉察中沦为被摆布的"提线木偶"[2]。

在一百多年前的工业社会,面对新闻媒体肆意侵扰个人私域生活的境况,学界首倡隐私权,自此"不被打扰、不受干预或控制"的愿景最终转化为一项独立的法律权利。进入到当今的信息社会,人类生产和生活日益数字化,大规模

隐私泄露或个人信息滥用问题层出不穷,隐私权保护逐渐上升为普遍的公共诉求,不再是局部的、零星的个人需求,人类的隐私权命运又一次站在十字路口。隐私权保护的失序意味着社会公序良俗的瓦解,很难想象现代人类文明在一个"彼此赤裸相见"、丧失理性思维和自由选择的原始形态中该如何接续。

隐私与个人信息虽有差别,但存在极其紧密的内在联系,个人信息保护可被视为隐私权在信息时代所发展出的新维度与应用延伸[3]。在数字社会,个人信息的不合理使用或滥用在很大程度上就是构成对隐私权的侵犯,个人信息保护是隐私权保护的重要路径,脱离个人信息保护孤立地谈隐私权保护是不科学的,也是不切实际的。随着全球数字化联络的发展,个人数据的大规模跨境流动已成常态,以隐私所代表的信息自主不再是一个单纯的法律问题或内政问题,更深切关系到国家的数据主权与信息安全,如2021年7月份的"滴滴事件"。① 因此,数据隐私的保护或控制领域成为世界各国争夺的重要阵地,这将直接影响自身数字经济的发展以及国际竞争的格局。

二、"名在实亡":悬崖边的隐私权

进入以数据流动为特征、以智能连接为纽带的数字社会,信息隐私可被大规模抓取或传播,无孔不入的智能监视技术正驱动着新的社会控制。而作为产生隐私危机主要场域的数字市场,调节机制基本失灵,个人隐私信息成为各方争夺的对象。隐私权虽仍存于纸面上,但在具体数字实践活动中被冲击殆尽,生存境遇岌岌可危。

(一)技术壁垒消解:普遍的隐私危机

在前工业化时期,信息传播的载体非常有限,传播的方式较为单一,技术也较落后。在这一时期,信息传播速度慢、受众范围小、空间距离短,加之当时信息的传播往往是伴随着人的流动而产生的,在人员流动缓慢且不频繁的状态下,信息传播很难形成一个规模性市场。即便信息隐私被泄露,也较容易在特定时空范围内采取物理手段进行控制或销毁。进入工业社会,传播技术飞速发展,电报机、电话机、电视机等的发明实现了信息的远距离快速传输,其规模化的普及使得大面积、远距离、跨地域传播成为现实,打破了信息传播原始的时空、受众、速率限制。尽管传播技术获得极大进步,然而侵犯隐私信息仍需通过人力或物理方式进行,如跟踪监视、布线窃听等,风险高、代价大、效率低。况且隐私信息窃取主要基于特定的政治、军事目的以及针对特定对象,影响范围相对有限,不至于引发较大的社会舆论反噬。可以说,在前信息社会,威胁隐私的力量还不够强大,仍存在各种有形或无形的技术瓶颈,且对象具有一定的指向性,隐私问题并不会演化成严重的社会危机[4]。

进入数字社会,信息的生产、分发与消费发生了根本性变革,信息的生产者、传播者、接收者三种角色逐渐融为一体,传播中的"知沟"或"数字鸿沟"不再是困扰传播两极分化的突出问题。如果说,前数字时代的传播方式是人力传播、电频传播,那么当今社会的传播就成为数字传播或智能传播,互联网、大数据、人工智能等是这一时期的显著特征。数据的融合应用驱动各行各业走向数字化、网络化与智能化,人类几乎所有的活动均能够以数字化的形式记录下来并加以利用,传统的隐私保护方式,如加密、去标识化、匿名化等,在"用户画像""人脸识别""自动化决策"等智能技术面前毫无招架之力,在当事人毫无察觉且不留任何外力痕迹的情况下,信息隐私即已移转[5]。在数字传播中,信息隐私不再是孤立的点,而是集群立体式的,且可以随时产生、实时更新、深度结合[6]。智能技术不仅可以直接抓取到用户的初始隐私,甚至可以对已公开的看似无关、分散、零乱的数据信息,通过深度结合与智能连接等手段挖掘出隐藏在面纱背后的个人隐私[7]。社会分工的细化

加深了个人对社会整体的依赖,且“生物个体”向“数字个体”的转向使人的自我隔绝寸步难行,要享受到数字社会的便利与福祉,用户不仅要让渡个人信息乃至隐私,还会在活动过程中时刻产生个性行为数据,大量用户的多维数据汇集成数据海洋,让数据的搜集、分析、处理、利用成本大大降低,获取“全本”而非“样本”数据的目标基本已无技术壁垒。隐私权保护问题的公共化反映的是隐私危机的无差别化与规模化,这与信息几乎无障碍流动与共享密切相关,在共享过程中,个人信息流转方向多变,保护难度系数增大,个人敏感信息泄露的概率骤增。大众传播在数字社会产生了革命性变化,速度的实时性、内容的海量性、形态的多媒体性、检索的便利性、过程的交互性、范围的全球性使信息传播达到了极致,信息隐私的泄漏动辄以千万级为单位计算,保护隐私的努力在强大的传播技术面前望尘莫及,普遍性的隐私危机开始出现[8]。

(二)超级全景监狱:无感的监视社会

英国著名功利主义思想家边沁构想了一种“全景敞视主义”社会管理手段;法国哲学家米歇尔·福柯在此基础上提出“中央监控式全景监狱”设想;美国学者马克·波斯特根据后现代语境下的技术统治霸权,提出“超级全景监狱”这一新型统治模式[9]。英国作家乔治·奥威尔在其政治寓言小说《1984》中所构思的一个对人民生活进行无孔不入的监视与操控的极权形态,在数字社会得到了某种程度的重现。在这一社会,私人空间与公共空间的界限不断消融,人们时时刻刻都处在被监视、窥探与把控中。在数字空间,个人已被自动生成为数字 ID,每一次行为痕迹都在“第三只眼”的窥视之中,形式多样的监视技术深入日常生活的各个角落,注册用的个人身份信息、点击浏览习惯、偏爱嗜好、行动轨迹等私密数据随时可以突破限制被搜集或利用。数字时代的物理时空消解、主权边界模糊、国家—社会混同、生物—数字的双重人性等社会趋势,使得隐私保护面临前所未有的威胁[10]。算法权力日益强大,无方向的监控大规模扩张,数据掌控的严重不对称,使得公众极易被掌控或支配,并产生意想不到的损害性结果[11]。数字社会的隐私权侵犯早已超越传统范畴,波及群体广泛,牵涉社会生活的诸多方面,若以一般标准或规范及以个体常规私权理念应对则显得过于单薄无力。

数字社会是一个高度依赖数据资源进行管理和控制的社会,与奥威尔极权式的压迫性服从不同,数字社会的监视是一种去中心化的监视,依靠诱惑性的引导对人的行为进行潜移默化式重塑,使之成为信息资本的“顺民”[12]。互联网平台企业强制授权、过度索取、超范围搜集个人信息几乎不受限制,致使用户非常容易被追踪而变得如此透明[13]。而且,即便信息隐私被侵犯,当事人可能还蒙在鼓里,“无感伤害”症状明显。在数字社会中,最前沿的数据使用技术及数据交易活动基本来自商业领域,为达到特定目的,公共部门也频繁与具有技术和市场优势的商业机构合作。2013 年曝出的美国棱镜计划(PRISM)深刻揭露了政府机构联合互联网巨头利用庞大的监视机器摧毁隐私以及互联网自由这一残酷现实,这昭示着公民隐私权在现代信息社会遭受多方强大力量围剿时是多么脆弱而无助。

(三)市场力量失灵:虚幻的保护承诺

隐私权保护不仅是一个法律问题,也是一个市场决策问题,无论个人、数字平台还是监管机构,均需对隐私权保护的成本和收益进行权衡,以实现最合理的隐私信息公开边界。然而,相较于生命健康权等不可克减性类人权,隐私权具有可被减损的伸缩特性,这使得隐私权保护在不同语境中存在较大的弹性空间[14]。对个人信息的挖掘使用是数字经济运转的必然要求,搜集的信息越具私密性或私密关联性则信息的准确性就越高,就越能获得巨大的经济效益。而且,数字社会的信息早已突破其传播沟

通功能,以代码形式成为一种权力与资源要素,谁掌握的信息越多,谁的权力就越大,谁就更能在激烈的市场竞争中占得先机或优势性地位。故而,效率、便捷、创新等价值因素考量被摆在优先选择和发展的位置,隐私权作为不得打扰、干预或限制(或禁止)传播个人信息的权利,在与上述价值的对抗中经常处于弱势地位,甚至被迫作出一定的妥协或牺牲。

智能信息技术的革命使得互联网发展成为公共基础设施,数字社会个人生产和生活的方方面面与互联网平台牢牢绑定。作为权力结构中心的数字平台,虽然基本由私营机构掌握,在市场环境中参与运营竞争,却扮演着社会公器的角色。有学者将隐私保护看作个人的理性经济决策问题,认为市场机制可以实现个人隐私的最佳保护[15]。然而,个人(用户)并非如百度CEO李彦宏所说的"愿意用隐私交换便捷性和效率",而是在数字语境中,个人在与数字平台企业的隐私谈判上存在明显的力量不对等,个人只能在"要么接受、要么走人"的选项中选择其一,几乎没有议价的空间[16]。如若选择进入数字平台享受服务红利,个人就必须让渡隐私信息,而个人信息一旦进入数字空间,基本上就会脱离原力束缚。信息搜集处理的不透明使得用户对其个人信息在何时间、以何方式、在何程度被搜集使用以及是否被转让或被第三方共享等情况很难知晓,用户在隐私决策上面临严重的信息不对称。即便是业界过度倚重的知情同意原则也并不能为个人隐私信息提供实质性保障,高昂的阅读成本与晦涩的术语词汇使得用户难以充分评估信息被披露的后果,导致知情同意沦为一种"非真实的意思表示",在具体实践中屡屡成为数字平台应付舆论危机的"挡箭牌",甚至成为违法搜集、处理用户信息的"合法依据"[17]。有学者对我国500家颇具影响力的网站的隐私政策声明(含个人信息保护政策)进行实证研究,发现70%的敏感信息类网站存在中级以上的隐私保护漏洞,大部分平台网站虽然发布了隐私政策,但现实中并没有采取相应措施兑现保护承诺,无法对用户的隐私安全产生实质性作用[18]。在数字市场中,数字平台正在深刻塑造而非简单反映社会行为规范,具有极强的主导作用,即便监管机构基于技术创新等因素进行考量,尽量避免过多干预,用户(数据主体)也近乎成为附庸,基本丧失真正的选择权与自主权。在如此失衡的环境中,隐私保护的失灵也就可想而知了。

三、域外规则:欧美模式中的隐私保护

当前隐私权生存境遇的危急非"一日之寒",长达数十年的信息技术发展与普及应用深刻改变了社会权力结构与互动模式,使隐私权不断遭受侵蚀。而智能科技的革命性突破则急速将我们的隐私权命运推向不可知与不可控的境地。面对隐私保护的严峻挑战,欧美凭借长期积累的先发优势率先走在前面,分别发展出不同风格的制度体系,并成为影响全球个人数据隐私权保护规则形成与演变的两大主流模式。

(一)欧盟:从隐私保护走向个人数据保护

隐私权在二战后得到空前重视,《世界人权宣言》(1948)确立了隐私权为人之基本权利,② 随后的《欧洲人权公约》(1950)关于公民隐私权遵循着类似的范式。③ 尽管如此,作为基本权利的隐私权并未在欧洲诸国得到充分展现。以大陆法系为代表的法国、德国为例:法国法不存在隐私权,其《法国民法典》第9条规定的"私生活受尊重权"于1970年才由立法加入进去,且该权利与肖像权等其他权利未严格区分;德国的民法与宪法并无隐私权概念,对隐私的保护主要依靠《德国民法典》第823条第1款作为"其他权利"的"一般人格权"来实现,是一种侧面或间接的保护[19]。而普通法系的英国在立法与司法传统上一直不承认存在独立的隐私权,隐私只有在与其他权利救济结合起来时,才能附带受到保护[1](P192)。直到2008年的马克思·莫斯利(Max Mosley)隐私权案,才让英国首次确

认了隐私权的独立存在(注:此时英国尚未脱欧)。④可以看出,虽然欧洲传统对以隐私为代表的人格尊严的维护比较重视,但并未建构起相应发达的隐私权保护体系。

20 世纪六七十年代,随着第三次科技革命的深入以及计算机的应用,欧洲开始注意到个人信息的使用与滥用问题,随之立法资源逐渐倾斜至个人信息/数据保护方向。以黑森州(联邦德国)颁布的世界首部《数据保护法》(1970)为开端,联邦德国与欧洲其他国家陆续颁布了类似的《数据保护法律》,⑤而后随着欧洲的一体化,最终形成了统一的《数据保护指令》(DPD,1995)与《数据保护条例》(GDPR,2016)。欧盟在个人数据保护制度产生之初时仍与传统的隐私保护制度纠缠,出现概念混用、认知不清等问题,随着时间的推移,二者逐渐区别开来且日益分工明确。DPD:同时使用隐私保护与数据两个概念→《欧盟基本权利宪章》(2000):将个人数据保护权从隐私权中独立出来→《里斯本条约》(2007):完全采用个人数据概念→GDPR:只有个人数据保护概念,不再使用隐私保护概念[20]。循此演进脉络可以看出,欧盟没有对隐私权进行改革,而是另行建构独立的个人数据保护制度体系,将之打造为隐私保护与个人信息保护的主导性机制。

欧盟把数据保护置于人权保护同样的高度,目的是保护人权法或宪法意义上的"个人基本权利"。欧盟数据立法的逻辑是:个人数据乃人之延伸,体现个人意志,应由数据主体掌控,否则就是对其不尊重[21]。人的尊严为欧盟个人数据保护理论的基石,暗含个人对个人数据及其处理的控制权。在该权利话语中,人之尊严维系优先于数据自由流动[22],力求通过综合性立法打造全面的数据保护网络,在此背景下制定的 GDPR 被普遍认为是国际社会最完善的数据保护立法。GDPR 对数据处理的所有关键环节加以严密规制,将个人数据的保护力度提升至前所未有的强度[23]。其对数据主体进行细致全面的赋权,对自动化决策行为进行严格限制,对任何滥用个人数据的责任主体进行严厉惩罚[24]。此外,GDPR 采取了以严格监管为核心的体制,设置欧盟数据保护委员会(EDPB)作为数据监管的最高权力机构,对成员国监管机构的成立、职责、权限等进行了详细规定,要求处理数据的企业或组织配备专门的数据保护专员(DPO),从而构建起自上而下的监管体系,并将公共部门和商业机构的数据使用行为纳入监管范围。

(二)美国:"大隐私权"中的个人信息保护

隐私权在美国诞生,经威廉·普罗斯的总结优化,形成了美国侵权行为法上的隐私权(privacy torts)。⑥1965 年,在"格里斯沃尔德诉康涅狄格州"(Griswold v.Connecticut)案中,美国联邦最高法院首度正式肯定隐私权系受宪法所保障的权利,创设了宪法上的隐私权(constitutional privacy)[25]。保障范围分为:个人自主决定(生育、婚姻、家庭、性关系等)与信息隐私。美国对信息隐私的保护按照行业属性(如通信、金融、教育、保险、儿童网络隐私等)采取分散(部门)立法模式,没有联邦层面的统一法典。可以看出,美国的隐私保护体系为:侵权行为法上的隐私权+宪法上的隐私权+信息隐私部门法。美国将个人信息保护纳入隐私保护的范畴,进而发展出发达的隐私权保护体系(可称为"大隐私权")[21]。作为普通法系国家,美国不存在大陆法上的人格权理论和制度,其隐私权早已脱离单纯的法权属性,成为一项宏大的制度安排。

与欧盟"直线式"(自上而下式)的个人数据保护立法实践不同,美国在个人信息保护立法上则是一种"条块式",即采取"联邦立法+州立法+部门专项立法"的模式。相较于欧盟在个人数据保护上表现出来的"严防死守"姿态,美国更关注个人数据的经济特性与商业价值,采取积极利用的态势,隐私立法以促进数据自由流动为原则[26]。数字企业在美国运营受到的

约束比欧盟要少,只要设置合理的内部合规要求与问责机制,就能较自由地开展业务或推出产品[27]。代表美国最新隐私保护理念的《加州消费者隐私法案》(CCPA,2018)虽为州级法律,但是鉴于加州作为美国经济第一大州以及州内数量众多且强大的互联网企业影响力,CCPA对美国乃至全球的信息隐私立法具有举足轻重的传染作用。CCPA规范的重心是商业行为,而非欧盟式的数据控制,注重发挥市场机制的基础性作用以促进数据开放共享,鼓励企业用经济手段平衡隐私保护与数字经济发展[28]。对个人数据保护的监管,美国主要依靠特有的业界自律模式,以实现公共机关对企业的最小化干预,这与美国的自由主义传统相契合。美国并无专门的数据保护官方机构,行使这一职能的主要是美国联邦贸易委员会(FTC),其在数据安全和隐私保护方面有着非常广泛的权力,对数字企业具有较强的震慑力,它与业界自律模式的结合构成美国独特的个人信息保护监管体系。

(三)欧美隐私权的弱化与隐私保护的坚守

如上文所述,隐私权在现代文明社会极其重要,但社会形态的迭代使其无法充分发挥预期功效。尤其是进入数字社会后,隐私权的结构性缺陷呈指数级放大,无法通过自我立法完善予以弥补,而只能另辟道路进行时代回应。从欧美的隐私权与个人数据保护生发演化轨迹来看,隐私权虽然起步相对较早,但作为一项人格权,所存在的先天局限性(封闭性、对世性、防御性)从根本上决定了其难以和数字社会完美兼容,致使其扩展空间相对有限。反倒个人数据保护立法正如火如荼地展开,成为当今全球最瞩目的立法运动,深刻影响着数字社会的行为规范。面对信息技术革命给隐私权保护带来的新问题与新挑战,欧美早早放弃了隐私权的场域主导地位,着力发展个人数据保护立法。无论是欧盟打造的"综合性"立法体系还是美国实行的"分散式"立法模式,均已在隐私权外另辟出独立运行的个人数据保护体系,设置了全新的制度程序与执法机制,使之成为保护隐私权的第一顺位防线,以承接数字时代信息隐私保护的重担。

四、中国路径:理念衡量、制度安排与立法缺憾

我国数字化应用已深入到社会生活的方方面面,颠覆性新技术塑造了新的社会形态,从信息社会进入透明社会发生在旦夕之间。面对严峻的隐私权保护态势,我国采取与欧美类似路径,淡化隐私权色彩,突出个人信息保护法等法律作用,初步建立起个人信息保护机制,但所遗留的一些关键问题仍需我们高度重视。

(一)绝对隐私与绝对保护的破除

李永军把个人信息区分为纯粹的个人隐私、隐私性信息、纯粹的个人信息,认为不同的个人信息具有不同的意义[29]。在此基础上,有些学者认为并非所有的隐私都具有同样的价值、且都要倾注同等的注意力,需对各类隐私进行价值分层并采取不同的保护举措[4]。在静止状态下此种区别对待可能存在一定的合理性,但在数字社会,信息隐私是一个动态而非固定的事物,同时,数字技术具有极强的信息重组与深度挖掘能力,很多看似无私密性的、公开的个人信息经智能整合与分析后会触及到背后所掩匿的隐私。另外,隐私并不存在严格意义上的客观标准与范畴,其随着人类活动在公私领域之间的变化而不断变动。故而,隐私的确定应结合具体的使用场景,无论立场预设抑或期待明确均不能绝对化,否则容易走向形而上学的极端,隐私看似有边界实则无边界。

隐私的边界深刻影响着隐私权保护的努力方向。在万物互联的智能社会,每个人都是行走的信息散发源,信息流动与变化难以预测,运行结果具有开放性,加之现有市场机制的不完善,导致隐私权保护具有高度的不确定性与随机性。此外,数字社会的隐私权保护亦牵涉一

个投入产出比问题。根据一项技术调查,随着低代码概念的兴起,当前 APP 的研发越来越趋向于结构化、模块化、低耦合化,通过模块整合方式所开发的 APP 最大的问题在于无法控制各个模块对个人信息搜集的行为[30]。而且,个人信息的处理存在漫长的活动链条,包含信息搜集、存储、使用、加工、传输、提供、公开等,所有环节由单一主体全程控制几乎没有可能性,每个环节甚至可能存在 N 个处理者,这使得个人信息的处理始终无法形成闭环,信息安全与隐私全程存在风险。若追求绝对的隐私保护,且不说是否具有技术可行性,低效的产出亦会使该努力难以为继。国家将数据定位为生产要素之一,⑦意味着数据除了具有个体属性外,还是可社会化配置和利用的经济资源。过度的隐私保护会扭曲市场机制并阻碍数字经济创新,既不能提升公众福祉,也无法实现经济社会最佳保护目标[31]。我国当前最重要的使命是促进数字产业的创新与发展,实现数字技术革命的弯道超车,在此基础上给民众带来更便捷更广泛的技术福利,这就决定了我们需要一个较宽松的数据法律与市场环境。如何促进数据资源分享与流通利用成为数据要素市场建设的核心,也是我国正在寻求的制度性突破所在。《中华人民共和国数据安全法》(以下简称《数据安全法》)(2021)第 7 条对此作出原则性回应。⑧而《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)(2021)仿效 GDPR 强化信息主体的权利,未充分顾及数据处理者(控制者)的合法利益,在促进数据流通分享与合理利用上存在一定的保守性[32]。尽管如此,除少数敏感与特殊领域,绝对的隐私与绝对的保护已基本被摒弃,隐私保护随个人信息保护进入“实用主义”阶段。

(二)以“大隐私权”涵盖“小隐私权”的局限

隐私权在传统市民社会与现代数字社会存在截然不同的生存境遇。在前数字时代的隐私权框架中,法律虽然偏向于对个人隐私提供“绝对”保护,但隐私权利范围相对有限,而且是一种被动的保护。在美国侵权法中,当存在触及威廉·普罗斯所归纳的四种隐私侵权类型且当事人提起诉讼时,相应的法律救济机制才会启动。在我国,隐私权作为私法上的人格权,遵循“不告不究”原则,国家机关一般不会主动介入民事主体间的隐私侵权纠纷。传统隐私权所面对的是市民社会的“熟人伤害”或“看得见的伤害”,能进入法院裁决的隐私侵权案件主要是常规隐私以及信息泄露的实质性损害案件[33]。而数字社会隐私侵权已发生翻天覆地的变化,其中一个重要特征是“无感伤害”,且主要作用于群体层面,大数据技术严重腐蚀了传统隐私权的范式基础,全方位瓦解了个体权利主张。可以说,传统隐私权是一种“小隐私权”,对普通个体的常规隐私纠纷可能会发挥作用,但面对数字社会的隐私危机时就会效力有限,既不能有效预防侵权行为的发生,也无法有效惩戒、威慑违法者。

在数字应用世界,人只是一个节点,数字平台所关注的并非特定个体数据而是大规模的集成数据,算法决策无需人的参与而可自主运行[34]。数字社会的数据是最重要的隐私载体,隐私保护与大数据处理过程紧密相关,单纯依靠传统的空间或心理上的排斥与对抗既不可行也不能行,这决定了无法采取以前防火墙式的静态保护,数据主体必须参与和融入数据的流动过程中,实行谦抑性动态保护。当今全球,包括欧美在内的主要法域国家或组织纷纷制定或修订个人数据保护法,确立大数据隐私法益,不再扩展侵权法中的隐私权,权利范式逐渐从隐私权过渡到个人信息保护,个人信息保护代替隐私权成为隐私保护的首位阵线。我国于 2012 年开始引入个人信息保护制度,之后《消费者权益保护法》(2013 修正)、《网络安全法》(2016)、《电子商务法》(2018)等包含个人信息保护的法律、法规、规章密集出台,隐私保护的主要任务逐渐转移至由个人信息保护承担,建

立起“保护隐私+保护个人信息不被滥用或不合理使用”双轨任务制。尽管如此,仍有学者建议通过变革传统侵权法,例如倒置举证责任、降低证明标准、设立公益诉讼,以对个人信息进行保护[35]。然而在数字社会,隐私保护乃至个人信息保护需要体系化的力量,寄希望于某个法律的修补、依靠单方面作用可能并不会达到预期效果,这可以在上述欧美法律的演进中得到明证。除维护自然人的合法权益外,个人信息保护在很大程度上所体现的是对公共利益与公共秩序的维系,主要保护机制应是公权规制而非个体诉讼和司法保护[27]。一个普遍趋势是以隐私权为原点开展个人信息保护,弱化传统隐私侵权诉讼的救济功能,将保护阵线前移,由被动防御转向主动规制,由纯粹的“事后救济”转变为“事前预防+事后惩戒”的二元模式[36]。我国基本上也采用此路径,正打造由《网络安全法》《数据安全法》《个人信息保护法》等法律法规构建的“大隐私权”体系,以覆盖“小隐私权”无法触及的领域。这些专项立法具有强烈的行政公法属性,通过禁止性或指引性规则辅以数据保护监管机构与责任惩戒机制,主动应对大数据处理过程中的隐私风险,保障数据主体的信息隐私。

(三)亟待解决的关键问题

第一,法律体系结构混乱。《中华人民共和国民法总则》(以下简称《民法总则》)(2017)发布之前,私法领域没有规定个人信息保护的内容。个人信息主要由行政法、刑法等公法予以保护。当然,若因侵犯个人信息造成权利人私法权益损害的,仍可适用侵权责任法的规定。在这一阶段,个人信息保护与隐私权之间存在清晰的关系脉络:一是平行适用,各负其责;二是梯度递进,个人信息较隐私权受到更高程度(更严格)的保护[37]。《民法总则》第111条关于个人信息保护的规定属宣示性条款,并未改变之前的关系格局。而《中华人民共和国民法典》(以下简称《民法典》)(2020)将个人信息保护与隐私权并列放在“人格权”编,不仅在结构上存在交叉,还出现内容交叉(第1032、1033条)与规则交叉(第1034条)。这些交叉还存在明显的种属混乱与法理冲突,例如,类属于个人信息的姓名、肖像、隐私等下位概念与个人信息这一上位概念并列在同一编,存在混乱的种属关系:上位概念的个人信息是权益而非权利,而下位概念的姓名、肖像、隐私则是权利,存在难以自洽的法理冲突,并且将隐私权保护逻辑适用于个人信息保护,在权利定性上也出现交叉错位。隐私权是一项传统的私法权利,而个人信息保护则是一项新型公法权益,在保护客体、义务主体、权利性质、责任救济等方面存在特殊性,有其独立的法律渊源、制度程序与执法机制[20]。将个人信息保护纳入人格权范畴,以传统的私权话语体系界定公法权益,无疑将模糊个人信息保护的权属基础,削弱其核心职能。可见,在法律体系结构上将个人信息保护纳入“人格权”编存在较大的弊病。

注意到上述问题后,《个人信息保护法》正式文本在第1条新加入“根据宪法,制定本法”的规定。这对《个人信息保护法》而言,意义重大。虽然从法源上讲,个人信息受法律保护源自宪法对公民人格尊严的保护,但立法上率先进行回应的却是私法上的《民法总则》以及承继它的《民法典》。在《民法典》之后制定《个人信息保护法》,容易使它被理解为实施《民法典》“人格权”编中“个人信息受法律保护”之规定的法律,被视为《民法典》的附属法律。而增加“根据宪法,制定本法”的规定,将使《个人信息保护法》成为实施宪法、保护公民基本权利的法律,被明确为一项独立的单行法,避免了个人信息保护的私法化。虽然上述修补在法理层面比较合理地解决了《个人信息保护法》制定的法源问题,使其脱胎初始即纠正了方向,但在法律体系结构上并未有根本改观,给法律的科学适用带来隐患。

第二,“碎片化”立法。欧美较早进入信息

化社会,从保护隐私向保护个人信息转轨的过程中积累了比较丰富的理论与实践经验,建构起转承平稳、逻辑严密、体系分明的个人信息保护机制。我国自 2012 年首次引入个人信息保护制度至 2021 年正式出台《个人信息保护法》,以不到十年的时间走完了欧美几十年的立法历程,这固然是可喜的进步,但时间上的压缩难免在体系质量上存在一定的问题。根据一项统计,在《个人信息保护法》出台前,我国有近 40 部法律、30 余部法规以及近 200 部规章涉及个人信息保护[38]。法出多门,规定零散,看似类似于美国的"分散式"立法模式,实则为"碎片化"立法,且相互之间多有重叠或缺漏之处,减损了立法的权威性以及管理的有效性[39]。《个人信息保护法》作为数字时代的基本法,虽已出台,但其体系内部的重复性与离散性问题还是当前亟待处理的问题。

第三,法律衔接不畅。个人信息保护要建构一套宏大的制度体系,除应发挥《网络安全法》《数据安全法》《个人信息保护法》三大支柱法的主导作用外,还需其他法律的支撑与补充。对于个人信息权益遭受损害后如何获得救济,《网络安全法》与《数据安全法》仅作出原则性的规定。⑨《个人信息保护法》第 69 条、第 70 条虽引入了民法中的侵权责任与诉讼法中的公益诉讼机制,但仍旧相当笼统,缺乏清晰明确的可操作性规则。如何建构个人信息保护法与民法、诉讼法等法律的衔接机制,在惩戒措施之外充分救济个人信息权益,仍有待进一步的科学立法设计。

五、结语

数字时代隐私权的全面弱化已成为不争的事实,而隐私权所维系的价值依然是我们人类的核心,面对愈演愈烈的隐私危机以及不断收缩的隐私权,个人信息保护制度逐渐填补领域空白,进阶为隐私保护的主导机制,并成为不可逆转的趋势。可以说,隐私权"神在而形移",原本应履行的职责使命转由个人信息保护承担。当前及今后,我们工作任务的重点是持续优化个人信息保护机制,构建完善的个人信息保护监管体系,以更好地应对数字技术对隐私权的挑战。

[注释]

① 2021 年 6 月 30 日,滴滴在纽交所挂牌。同年 7 月 2 日,国家网信办发布公告,对"滴滴出行"实施网络安全审查,并暂停了其新用户注册。7 月 4 日,调查结论出炉,指控滴滴严重违法违规收集客户个人信息,通知应用商店下架滴滴出行 APP。7 月 16 日,国家网信办会同公安部、国家安全部、自然资源部、交通运输部、税务总局、市场监管总局等部门联合进驻滴滴出行科技有限公司,开展网络安全审查。

② 《世界人权宣言》第 12 条规定:任何人的私生活、家庭、住宅和通信不得任意干涉,他的荣誉和名誉不得加以攻击。

③ 《欧洲人权公约》第 8 条规定:人人有权享有使自己的私人和家庭生活、家庭和通信得到尊重的权利等。

④ 2008 年 3 月,《世界新闻报》刊载了时任国际汽车联盟主席的莫斯利"狂欢派对"的图文报道,并将相关视频上传至网站进行传播。莫斯利针对上述视频的传播向法院申请禁令被拒绝后向法院起诉,要求确认《世界新闻报》侵犯其名誉权、隐私权。经过审理,英国最高法院宣布《世界新闻报》因侵犯莫斯利名誉权、隐私权而败诉。

⑤ 例如,《瑞典数据法》(1973)、《德国联邦个人数据保护法》(1977)、《法国数据保护法》(1978)等。

⑥ 1960 年,美国侵权行为法学者威廉·普罗斯(William L. Prosser)总结提出四种隐私侵权类型:侵入原告的私密领域;曝光原告令人难堪的私人事实;不合理的曝光致使他人遭受公众误解;出于私利盗用他人的姓名或肖像。

⑦ 2020 年 3 月 30 日发布的《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》将数据定位为五大生产要素之一,与土地、资本、劳动力、技术并列。

⑧ 《数据安全法》第 7 条规定:国家保护个人、组织与数据有关的权益,鼓励数据依法合理有效利用,保障数据依法有序自由流动,促进以数据为关键要素的数字经济发展。

⑨ 《网络安全法》第 74 条与《数据安全法》第 52 条均规定:违反本法规定,给他人造成损害的,依法承担民事责任。

[参考文献]

[1] 王泽鉴.人格权法:法释义学、比较法、案例研究[M].北京:北京大学出版社,2013.

[2] 邵国松,黄琪.算法伤害和解释权[J].国际新闻界,2019(12):27-43.
[3] 石佳友.隐私权与个人信息关系的再思考[J].上海政法学院学报,2021(5):81-98.
[4] 董淑芬,李志祥.大数据时代信息共享与隐私保护的冲突与平衡[J].南京社会科学,2021(5):45-52,70.
[5] 邵国松,黄琪.人工智能中的隐私保护问题[J].现代传播(中国传媒大学学报),2017(12):1-5.
[6] 范海潮.作为"流动的隐私":现代隐私观念的转变及理念审视——兼议"公私二元"隐私观念的内部矛盾[J].新闻界,2019(8):59-69.
[7] Ira S.Rubinstein.Big Data:The End of Privacy or a New Beginning?[J].International Data Privacy Law,2013,3(2):1-14.
[8] 郭庆光.传播学教程(第二版)[M].北京:中国人民大学出版社,2011:107.
[9] 林爱珺,蔡牧.大数据中的隐私流动与个人信息保护[J].现代传播(中国传媒大学学报),2020(4):79-83.
[10] 马长山.数字时代的人权保护境遇及其应对[J].求是学刊,2020(4):103-111.
[11] 马长山.智慧社会背景下的"第四代人权"及其保障[J].中国法学(文摘),2019(5):5-24.
[12] 邵成圆.重新想象隐私:信息社会隐私的主体及目的[J].国际新闻界,2019(12):44-57.
[13] David C.Vladeck. Consumer Protection in an Era of Big Data Analytics[J].Ohio Northern University Law Review,2016(42):493-515.
[14] 廖丽,师亚楠.欧盟大规模数据监控的赋权、制衡与挑战[J].欧洲研究,2020(6):71-89,7.
[15] George J.Stigler.An Introduction to Privacy in Economics and Politics[J]. The Journal of Legal Studies,1980,9(4):623-644.
[16] 唐要家.中国个人隐私数据保护的模式选择与监管体制[J].理论学刊,2021(1):69-77.
[17] 范海潮,顾理平.探寻平衡之道:隐私保护中知情同意原则的实践困境与修正[J].新闻与传播研究,2021(2):70-85,127-128.
[18] 邵国松,薛凡伟,郑一媛,等.我国网站个人信息保护水平研究——基于《网络安全法》对我国500家网站的实证分析[J].新闻记者,2018(3):55-65.
[19] 郗伟明.论英国隐私法的最新转向——以Mosley案为分析重点[J].比较法学研究,2013(3):104-119.
[20] 周汉华.个人信息保护的法律定位[J].法商研究,2020(3):44-56.
[21] 高富平.个人信息保护:从个人控制到社会控制[J].法学研究,2018(3):84-101.
[22] 解正山.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[J].法商研究,2020(2):71-84.
[23] Karen Yeung. Making Sense of the European Data Protection Law Tradition[J].The London School of Economics and Political Science,2017:34-45.
[24] 国瀚文,李婷婷.数据要素政策指导背景下的隐私权保护研究[J].上海法学研究(集刊),2020,18:109-118.
[25] 曹鸿.节育与婚姻——美国"格里斯沃尔德诉康涅狄格州案"的社会政治史考察[J].兰州学刊,2016(8):96-105.
[26] Daniel Castro.The Rise of Data Poverty in America[J].Center for Data Innovation,2014:1-12.
[27] 刘泽刚.大数据隐私权的不确定性及其应对机制[J].浙江学刊,2020(6):48-58.
[28] 刘泽刚.大数据隐私的身份悖谬及其法律对策[J].浙江社会科学,2019(12):21-30,155.
[29] 李永军.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[J].浙江工商大学学报,2017(3):10-21.
[30] 彭根."零信任"的APP合规技术能力[EB/OL].https://mp.weixin.qq.com/s/LNtxZlzHwDtOUnvT4IiY8A,2021-08-03.
[31] 唐要家,汪露娜.数据隐私保护理论研究综述[J].产业经济评论,2020(5):95-108.
[32] 高富平.欧盟寻求救赎,中国难逃窠臼——"个保法"通过有感[EB/OL].https://mp.weixin.qq.com/s/CO0Gvm2j2qqNJOsRCjOIXA,2021-08-20.
[33] 李婷婷,张明羽.信息社会的隐私权利主张与司法回应——基于隐私侵权案由裁判文书的内容分析[J].国际新闻界,2019(12):85-107.
[34] 余成峰.信息隐私权的宪法时刻——规范基础与体系重构[J].中外法学,2021(1):32-56.
[35] 叶名怡.个人信息的侵权法保护[J].法学研究,2018(4):83-102.
[36] 张平.大数据时代个人信息保护的立法选择[J].北京大学学报(哲学社会科学版),2017(3):143-151.
[37] 周汉华.平行还是交叉:个人信息保护与隐私权的关系[J].中外法学,2021(5):1167-1187.
[38] 邵国松,杨丽颖.在线行为广告中的隐私保护问题[J].新闻界,2018(11):32-41.
[39] 彭诚信,向秦."信息"与"数据"的私法界定[J].河南社会科学,2019(11):25-37.