

# 个人信息私法保护的困境与出路

丁晓东\*

---

内容提要：关于个人信息法律保护的研究，当前的主流观点采个体主义的立场，将个人信息视为私权的客体，以域外经验为证，认为私法可以有效保护公民的相关隐私权益。实际上，域外的相关法律并未承认个人信息权有对抗不特定第三人的效力；在现代信息社会中，以私法保护公民的隐私权益也常遇到困难。对隐私权益必须进行场景化的理解，个人信息流通具有公共性价值。法律保护个人信息的目的在于防范相关风险，促进个人信息在具体场景中的合理流通。宜通过“消费者法化”，重新激发个人信息私法保护的活力；同时，采取公法框架进行风险规制，保护个人信息。

关键词：隐私权益 个人信息 私法保护 消费者保护 风险规制

---

当前，由个人信息的大规模收集与利用引发的社会问题层出不穷，必须加强个人信息的法律保护已经成为学界共识。然而，个人信息的法律性质如何界定？法律又当采取何种手段保护个人信息？针对上述问题，学界仍有争议。有学者认为，个人信息是一种人格性权益，应当适用人格权的法律框架加以保护；<sup>〔1〕</sup>也有学者认为，个人信息是一种财产性权益，应当适用财产权的法律框架加以保护；<sup>〔2〕</sup>还有学者提出，个人信息是一种新型的权利，需要在法律中增设个人信息权。<sup>〔3〕</sup>观点虽有分歧，但它们的前提假设却是相同的，即认为个人信息是具有排他性的私权的客体，应当通过以主体平等和意思自治为原则的私法

---

\* 中国人民大学法学院、未来法治研究院副教授。

本文系国家自然科学基金一般项目“大数据背景下的个人信息保护与企业数据权属研究”（18BFX198）的阶段性成果。

〔1〕 代表性的论述，参见罗昆《个人信息权的私权属性与民法保护模式》，《广西大学学报（哲学社会科学版）》2015年第3期，第88页以下。

〔2〕 代表性的论述，参见刘德良《个人信息的财产权保护》，《法学研究》2007年第3期，第80页以下。

〔3〕 代表性的论述，参见蒋怡《论个人信息权在民法中确立的必要性》，《昆明大学学报》2008年第4期，第5页以下；李伟民《“个人信息权”性质之辨与立法模式研究——以互联网新型权利为视角》，《上海师范大学学报（哲学社会科学版）》2018年第3期，第66页以下。

加以保护。这一前提假设很难成立。在比较法的视野下考察，域外的隐私权益<sup>(4)</sup>保护正经历着从私法主导到消费者法与公法主导相结合的变迁；从法律原理的层面看，传统侵权法已无力保护现代信息社会中的隐私权益，以个人信息权或财产权为基础保护隐私权益又面临着保护不足与保护过度的两难。

在保护个人信息方面，传统的私法进路之所以存在困境，深层原因在于隐私权益与个人信息的性质特殊。保护隐私权益并不意味着要隔断个人信息的流通，个人信息天然具有社会公共属性，并非一种具有固定边界的私人权利。现代社会之所以强化个人信息保护，原因在于个人不易对个人信息流通中的风险进行有效管理。面对越来越复杂的信息收集方式和信息的不规范流转，个人也很难对相关风险加以判断和防范。从上述事实出发，我国未来的个人信息保护立法应当侧重消费者法保护和公法保护的途径。一方面，为重新激活个人信息私法保护的活力，寻求个人信息私法保护的出路，应当将个人信息保护纳入消费者法的框架，在特定场景下对个体进行倾斜保护，确保具体场景中的信息流通满足消费者的合理期待。另一方面，应当建构网络、信息等特定领域的公法框架，通过风险评估和风险规制，为个人信息的合理流通与使用创造条件。

## 一、个人信息私法保护的核心观点

当前我国个人信息法律保护的研究中，将个人信息视作一种个体性的私权，主张以私法的框架对其进行保护的观点，得到了很多研究者的认同。<sup>(5)</sup>与之相关的两个核心论点也被广泛接受，对我国的个人信息法律保护研究产生了很大影响。

第一个论点是比较法上的事实判断：域外的隐私权益保护经历了从隐私权到个人信息权的演进，并且都采取了私法的保护模式。对于隐私权益保护的起源，大多数研究者都将其追溯到沃伦与布兰代斯的《隐私权》，指出其私法保护的特征。在这篇经典文献中，沃伦与布兰代斯认为，尽管被侵犯的隐私不受传统普通法的保护，但普通法仍应通过法官造法推论出隐私权这一法律权利，普通法法院应当将侵犯隐私作为侵权行为加以追究。<sup>(6)</sup>其后，美国的司法实践逐渐认同了沃伦与布兰代斯的建议，开始以侵权法的方式保护公民的隐私权益。侵权法学者威廉姆·普罗斯归纳的美国司法实践中四种隐私侵权，<sup>(7)</sup>亦被国内研究者广泛提及。<sup>(8)</sup>

(4) 本文所称的“隐私”或“隐私权益”并不等同于民法上的“隐私权”，本文使用的“隐私”或“隐私权益”是一个大隐私的概念。当下，“隐私”或“隐私权益”已成为全球互联网与信息技术领域的通用术语。包括中国在内的各个国家的网站和手机APP，在阐述其个人信息保护政策时，使用的都是“隐私”或“隐私政策”，而非“个人信息政策”这样的表述。

(5) 代表性的论述，参见严鸿雁《论个人信息权益的民事权利性质与立法路径——兼评〈个人信息保护法〉（专家建议稿）的不足》，《情报理论与实践》2013年第4期，第43页以下；张里安、韩旭至《大数据时代下个人信息权的私法属性》，《法学论坛》2016年第3期，第119页以下；王晓芬《个人信息的法律属性及私法保护模式探究》，《河南财经政法大学学报》2016年第5期，第64页以下。

(6) See Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

(7) See William L. Prosser, *Privacy*, 48 Calif. L. Rev. 383 (1960).

(8) 代表性的论述，参见方新军《一项权利如何成为可能？——以隐私权的演进为中心》，《法学评论》2017年第6期，第111页；前引(5)，张里安等文，第123页。

不少研究者指出,自20世纪60年代以来,美国法对于隐私权益的保护经历了从隐私权保护到个人信息权保护的转变。<sup>(9)</sup>阿兰·威斯丁于1967年出版的《隐私与自由》一书,被认为是一个关键性的转折点。在该书中,威斯丁不再满足于沃伦和布兰代斯对于隐私权的模糊界定,也不认同普罗斯以四种类型限定隐私侵权的做法。在威斯丁看来,以往对于隐私的定义都是模糊的,隐私必须被重新界定为“个人、群体或机构对自身信息在何时、如何以及在什么程度与他人沟通的主张”,<sup>(10)</sup>换句话说,隐私就是个人对自身信息的控制。

在一些研究者看来,德国和欧盟的隐私权益法律保护也经历了相似历程。这些研究指出,德国和欧盟一些国家的私法都曾将隐私归入人格权的范畴,以私法的方式保护隐私权益。到20世纪70、80年代,个人信息权或个人信息自决权的概念开始出现,成为受到法律保护的另一核心权利。也就是说,德国和欧盟对于个人信息法律性质的界定,经历了从隐私权到个人信息权的转变,个人信息的法律保护途径也从隐私权的私法保护过渡到了个人信息权的私法保护。<sup>(11)</sup>

第二个论点偏重法律原理与应然性判断,认为从法律原理出发,可以得出这样的结论:为了更好地保护公民的隐私权益,有必要在私法体系中明确个人信息权,确定个人信息权的边界。首先,目前我国旨在保护隐私权益的立法非常零散,大多数的法律规范针对的只是特定行业的特定个人信息。这些立法的层级、关注领域和调整模式均不相同,缺乏体系上的融贯性,没有对个人信息的性质进行明确界定,法律规范大多偏重宣示性地设定义务,缺少法律责任的规定,<sup>(12)</sup>因此有必要从私法的角度加强个人信息的法律保护。其次,针对现行隐私权益法律保护体系较为零散和缺乏融贯性的特点,需从私法上厘清个人信息的法律地位,从而为隐私权益提供更为集中和体系化的保护。再次,由于私人主体更有动力和积极性去维护自身利益,加强个人信息的私法保护,也有助于发动公民个体力量维护其自身权益。<sup>(13)</sup>

还有研究指出,我国私法对隐私权益的保护经历了从无到有、从只关注隐私权到同时关注个人信息权的变化。1986年民法通则没有规定隐私权,但两年后,最高人民法院的司法解释确认了个人隐私应受法律保护。<sup>(14)</sup>2009年侵权责任法第2条将隐私权明确规定为民法

(9) 代表性的论述,参见杨惟钦《价值维度中的个人信息权属模式考察——以利益属性分析切入》,《法学评论》2016年第4期,第68页以下。作者指出,随着美国“社会的发展和学说的跟进,在私法领域内隐私权被赋予了更加丰富的内涵,扩充为信息隐私权、空间隐私和自我决定的隐私”;60、70年代后,“美国的隐私权体系从防御性的权利向进取性的权利发展,强调主体对自身信息的支配、控制与决定”。

(10) Alan Westin, *Privacy and Freedom*, New York: Atheneum, 1967, p. 7.

(11) 代表性的论述,参见前引〔5〕,张里安等文,第122页以下;齐爱民《拯救信息社会中的人格》,北京大学出版社2009年版,第77页;彭礼堂、饶传平《网络隐私权的属性:从传统人格权到资讯自决权》,《法学评论》2006年第1期,第57页以下。

(12) 代表性的论述,参见郭瑜《个人数据保护法研究》,北京大学出版社2012年版,第43页以下;洪海林:《个人信息的民法保护研究》,西南政法大学2007年博士论文,第162页;杨咏婕《个人信息的私法保护研究》,吉林大学2013年博士论文,第415页以下。

(13) 代表性的论述,参见王鲁东《个人信息权法律保护探析》,《中共青岛市委党校(青岛行政学院学报)》2008年第10期,第93页以下;凌学东、鞠晔《网络消费者个人信息综合保护机制研究》,《兰州学刊》2016年第8期,第157页以下。

(14) 《最高人民法院关于贯彻执行〈中华人民共和国民法通则〉若干问题的意见(试行)》(1988年通过,已于2008年12月14日部分废止)第140条规定“以书面、口头等形式宣扬他人的隐私,或者捏造事实公然丑化他人人格,以及用侮辱、诽谤等方式损害他人名誉,造成一定影响的,应当认定为侵害公民名誉权的行为。以书面、口头等形式诋毁、诽谤法人名誉,给法人造成损害的,应当认定为侵害法人名誉权的行为。”

事权利，将隐私权纳入人格权的保护范畴。2017年民法总则不但在第110条中确认了自然人享有隐私权，还在第111条专门规定了个人信息受法律保护，在第127条中规定了对数据的保护。以上说明，加强个人信息的私法保护，符合我国隐私权益法律保护体系的发展趋势。<sup>[15]</sup>

综上，当前我国个人信息法律保护研究将个人信息视为私权的客体，且认为私法能够有效保护公民的相关隐私权益，这一结论的得出有赖于上述两个论点的成立：其一，在域外实践方面，个人信息法律保护的权利基础沿着从隐私权到个人信息权的路径发展，且未偏离私法保护的轨道；其二，在学理和国情层面，加强个人信息的私法保护乃是大势所趋，不仅具有必要性，也具有应然性。然而，以上对域外经验的解读和对法律原理的理解，实际上均存在一定的误区，无助于证成个人信息天然的私权属性，无法为个人信息保护的私法优位立场奠定基础。

## 二、域外经验的重新解读

关于域外隐私权益保护经历了从私法上的隐私权到私法上的个人信息权转变的观点，其实属于对域外经验的误读，经不起深入的推敲。

### （一）美国经验

初看上去，第一个论点的确描绘了美国隐私法的历史变迁。在美国隐私法发展之初，沃伦与布兰代斯、普罗斯都没有提及个人信息的概念，美国的法律实践也没有将个人信息作为一种法律权益的客体加以保护。20世纪六七十年代，威斯丁首先提出个人信息的概念，将隐私界定为个人对自身信息的积极性控制，随后，个人信息的概念才在美国隐私法中被广泛采用。

然而，在美国，个人信息的概念是在独特的技术背景之下，针对独特的防范对象提出的，并未成为一种可以对抗不特定第三人的权利。具体说来，个人信息概念的兴起以20世纪60年代以后计算机技术的兴起为背景。<sup>[16]</sup>计算机技术的兴起，使得公共机构和公司处理信息的方式发生巨变。在此之前，信息的收集主要依赖人工，信息收集的速度较慢；信息的储存主要通过卡片、文档等方式，且需要特定的储存点；信息的搜索主要依赖编码索引和人工查找，费时费力。计算机技术兴起后，信息的收集速度有了质的提升；信息的储存能力几乎没有上限，且不再需要特定的储存点；同时，信息的搜索也变得简单易行。在这样的背景下，美国政府采取了一系列加强个人信息保护的举措，美国国会也通过了一系列立法，致力于确保个人信息在特定领域不受侵犯。

分析美国政府所采取的一系列个人信息保护措施和美国国会的一系列个人信息立法，不难发现，这些措施和立法都集中于某些风险较大的领域，规制的对象是政府、学校、医院等大型机构及企业的大规模个人信息收集行为。例如，1973年美国医疗、教育与福利部

[15] 代表性的论述，参见常健《论人格权法（编）中的个人信息权的制度完善——评〈中华人民共和国民法典人格权编（草案）·民法室室内稿〉相关规定》，《四川大学学报（哲学社会科学版）》2018年第3期，第32页以下。

[16] See Arthur R. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers*, Ann Arbor, MI: University of Michigan Press, 1971.

首先推出了一份名为《记录、电脑与公民权的报告》。在这份报告中,美国医疗、教育与福利部将个人信息定义为任何可识别个人的信息,规定这些信息的收集、披露和使用都必须遵循所谓的“合理信息实践”原则。根据合理信息实践原则,任何收集和储存个人信息的系统都不得秘密运行;个人必须能够知道其哪种类型的信息是被记录的,哪种类型的信息是被使用的;个人必须能够阻止其个人信息被用于其不同意的目的;个人必须能够纠正或修改那些能够识别他个人身份的信息。<sup>(17)</sup>

其后,美国国会针对个人信息保护通过了一系列立法,这些立法也只适用于特定领域和特定对象。<sup>(18)</sup>以1974年的家庭教育权利与隐私法和隐私法为例。前者规定,对于教育纪录中任何可识别个人的信息,教育机构都有义务确保信息不被泄露,并且保证个人能够获取和修改其个人信息。<sup>(19)</sup>后者则要求,所有美国联邦规制机构在处理个人信息时都必须遵循相应规定,除有例外情况,规制机构在公开个人信息前必须取得个人的书面同意,个人有权访问其被联邦机构保有的个人信息并对个人信息进行纠正。<sup>(20)</sup>1984年,美国国会通过了具有里程碑意义的联邦有线通讯政策法。该法将可识别个人的信息作为核心概念,从信息的收集到信息的储存和使用,只要涉及可识别个人的信息,电讯公司就必须遵循一系列合理信息实践原则。此后,国会又分别通过了儿童网上隐私保护法、视频隐私保护法、司机隐私保护法,要求相应主体在特定情形下收集和使用个人信息的行为必须符合相关规定。

美国的个人信息保护措施和相关立法带有明显的消费者法保护或公法规制的特征。由于并未赋予个人以针对不特定第三人的权利,对于普通民事主体收集与处理个人信息的行为,这些立法并不适用。事实上,即使对于一般企业,美国的上述立法也大都无法适用。对于一般企业的隐私权益保护,美国法大体采取的是企业自我规制和消费者法规制的进路。<sup>(21)</sup>由企业自愿制定隐私政策,然后由美国联邦贸易委员会确认企业的隐私政策中是否存在欺诈或不合理的情形,以及企业是否严格执行了其隐私保护的承诺。<sup>(22)</sup>

分析威斯丁的《隐私与自由》同样会发现,威斯丁对于隐私与个人信息的探讨以计算机与现代科技的兴起为背景,并没有将个人信息泛化为一种私法意义上的权利。虽然威斯丁对隐私下了一个接近于个人信息权的定义,认为隐私是“个人、群体或机构对自身信息在何时、如何以及在什么程度与他人沟通的主张”,<sup>(23)</sup>但其所说的自身对信息的控制权主要针对的,是计算机、现代科技以及与此相结合的权力对个体的威胁,并没有以私法的视角看待“个人信息权”。在这本奠定现代信息隐私法的经典著作中,威斯丁只在几处蜻蜓点水式地引用了沃伦、布兰代斯的侵权文献,<sup>(24)</sup>对于普罗斯的侵权法分类,威斯丁根本没有

(17) <http://www.privacilla.org/government/hewreport.html>, 2018年11月3日最后访问。

(18) 在此之前,美国国会已经通过了公平信用报告法(1970)。该法规定,消费者保护机构评定信用以获取贷款和保险,必须遵循某些信息保护的规则,尽管这一法案尚未提出个人可识别信息的概念。

(19) 20 U. S. C. § 1232g (2006) .

(20) 5 U. S. C. § 552a (2006) .

(21) See Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 Penn St. L. Rev. 587, 593 (2007) .

(22) See Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 Admin. L. Rev. 127, 130-31 (2008) .

(23) 前引〔10〕, Westin文。

(24) 威斯丁在著作中提及沃伦与布兰代斯《隐私权》之处,参见前引〔10〕, Westin文,第346页,第348-349页,第355页。

提到。这从另一个侧面说明，威斯丁并没有继承沃伦、布兰代斯与普罗斯的侵权法传统，没有期望以侵权法或其他私法的框架来保护个人信息。<sup>(25)</sup>

## (二) 德国经验

在德国，对个人隐私的法律保护是通过人格权的私法化完成的。制定于1900年的德国民法典没有规定人格权或隐私权。二战后，德国联邦最高法院通过1954年的“读者来信案”确认了这一权利。该案判决认为，德国基本法第1条第1款所提到的个人尊严可以作为德国民法上的渊源性权利，<sup>(26)</sup>个体“作为人的尊严和发展其个体人格”的利益应当受到民法的保护，这一人格权可以对抗不特定第三人。<sup>(27)</sup>1958年，德国联邦最高法院在“骑士案”中确认了对伤害人格权行为的损害赔偿，认为对人格权的伤害与一般性的人身伤害同等严重。<sup>(28)</sup>1973年，德国联邦最高法院在“伊朗王后案”中最终确立了对个人隐私的人格权保护，法院认为基本法第1条和第2条保护了“个人的隐私领域”，个人有权“实现独处的愿望”，保持“自身不被外界打扰”。<sup>(29)</sup>

有学者认为，经过发展，德国不仅确立了隐私权益的人格权保护，而且确立了基于个人信息自决权的法律保护。<sup>(30)</sup>不少学者称，在“小普查案”和“人口普查案”等案件的基础上，德国已经确立了一种私法上的信息自决权，一种类似于威斯丁所定义的个人对于自身信息得以积极控制的基本权利：法律应当保障个人的知情权和选择权；只有在个人同意时，才能允许其个人信息被收集。如果信息收集者在个人不知情或表示拒绝的情形下收集个人信息，便构成对公民个人信息自决权的侵犯。<sup>(31)</sup>然而，上述观点的得出实际上是对相关案例的误读。德国联邦最高法院有关个人信息权的判决是在特定语境下作出的。“小普查案”和“人口普查案”的判决结果针对的是国家对于个人信息的威胁，法院并未将所谓的个人信息权或个人信息自决权扩展成为一种针对不特定第三人的私法权利。正如学者所言，德国法院对于个人信息自决权的正当化论证有其特殊的案件背景，“信息自决权的主张者忽略了这些案例的具体背景，扩大了核心表述的适用范围，从而也就使所谓的信息自决权脱离了正当化的基础”。<sup>(32)</sup>

同美国类似，德国有关个人信息或个人数据的立法也是在公法或消费者法的框架下进行的。1970年，德国黑塞州制定了第一部州层面的数据保护法。1977年，德国制定了《防

(25) 在这个意义上，可以说威斯丁对于隐私的界定标志着现代隐私法的诞生。威斯丁去世时，《纽约时报》撰文悼念，认为威斯丁“几乎以一人之力创立了隐私法”。See Margalit Fox, *Alan F. Westin, Who Transformed Privacy Debate Before the Web Era, Dies at 83*, N. Y. Times, Feb. 23, 2013, at D7.

(26) 对于此案的介绍，参见[德]迪特尔·梅迪库斯《德国民法总论》，邵建东译，法律出版社2013年版，第805页以下。

(27) 在德国法律理论上，这被称为“第三人效力理论”。对此理论的深入分析，参见陈新民《宪法基本权利及对第三者效力之理论》，载陈新民《德国公法学基础理论》上册，法律出版社2010年版，第349页以下。

(28) Federal Constitutional Court, BGHZ 26, 349, quoted from Paul M. Schwartz and Karl-Nikolaus Peifer, *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?*, 98 Cal. L. Rev. 1925 (2010).

(29) Federal Constitutional Court, BVerfGE 34, 269, 281, quoted from Id.

(30) 前引〔11〕，彭礼堂等文，第57页。

(31) 同上文，第58页。

(32) 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》，《比较法研究》2015年第6期，第26页。

止数据处理过程中滥用数据法》，并在其后进行了若干次修订。尽管人们认为，德国相关法律提供的隐私权益保护比美国更为严格，但其针对的对象、基本原则、保护手段同美国的相关立法仍然高度一致：这些法律针对的是个人信息或个人数据的收集者或处理者，而不是日常生活中的一般个体；这些法律大致遵循了美国1973年《记录、电脑与公民权的报告》中所归纳的合理信息实践原则；法律所提供的保护手段是对信息的收集、处理与使用过程进行消费者法与公法规制，并未诉诸私法上具有排他性的个人信息权。总的来说，这些法律并不保护个人数据本身，而是意在确保信息收集者在处理个人数据时不损害个人的隐私权益。<sup>(33)</sup>

### （三）欧洲其他国家与欧盟的经验

除德国外，欧洲其他国家也采取了消费者法与公法规制进路，为个人信息或个人数据提供保护。20世纪70年代，瑞典（1973）、奥地利（1978）、丹麦（1978）、法国（1978）、挪威（1978）等国先后立法，形成了第一波个人信息或个人数据立法潮流。<sup>(34)</sup>这些立法尽管各有不同，但基本都吸纳了合理信息实践原则，规制的是政府与企业对个人信息的处理过程。

在欧盟层面，有关个人信息或个人数据保护的立法也采取了类似进路。1980年，欧洲理事会制定了供成员国参照和选择适用的《个人数据自动化处理保护公约》。<sup>(35)</sup>1995年，欧盟通过了《欧盟数据保护指令》，要求成员国必须通过国内立法对其加以适用。2016年，欧盟又通过了《一般数据保护条例》，于2018年直接适用于欧盟成员国。在这些立法中，欧盟为保护个人信息或个人数据采取了越来越严格的监管措施，但其都是基于合理信息实践原则对信息的收集、处理、储存和使用进行的过程监管。欧盟并未创设一种私法上的个人信息权或个人数据权，更没有主张公民个体可以凭借个人信息权或个人数据权对抗不特定第三人。<sup>(36)</sup>有学者基于《欧盟基本权利宪章》第8条第1款的规定（每个人都有权使其个人数据得到保护）认为，欧盟已经在其中明确了个人信息权或个人数据权。这种看法是将个人数据得到保护的简单等同于个人数据权。实际上，个人数据得到保护的是一种派生于消费者法保护与公法保护的权益，而非一种一般性的私法权利。

从司法实践来看，欧盟也没有将个人数据得到保护的权益泛化为一般性的私法权利。例如，在2003年的一起案件中，针对奥地利立法机关作出的高级政府官员必须将其薪资告知审计机关的规定，欧盟法院并没有将高级官员的个人信息视为私法权利的客体，没有认为获取该个人信息的主体必须给予信息提供者以补偿。相反，法院直接援引了《欧洲人权公约》第8条的隐私权规定，分析了相关当事人的权利是否受到侵犯。<sup>(37)</sup>其后，在“西班牙

(33) See J. Lee Riccardi, *The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?*, 6 B. C. Int'l & Comp. L. Rev. 243, 248 (1983).

(34) See Colin J. Bennett & Charles D. Raab, *The Governance of Privacy: Policy Instruments in a Global Perspective*, Cambridge, MA: MIT Press, 2006, p. 127.

(35) Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, Jan. 28, 1981, E. T. S. 108, available at <http://conventions.coe.int/T/Eat/y/en/Treaties/Html/10>, 2018年11月3日最后访问。

(36) 《一般数据保护条例》的多项条款都表明了这一点，例如第2条第2段c项规定，“自然人在纯粹个人或家庭活动中所进行的个人数据处理”不适用《一般数据保护条例》。

(37) Case C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989.

牙音乐制造商协会案”<sup>(38)</sup>“萨塔梅迪亚案”<sup>(39)</sup>“巴伐利亚啤酒案”<sup>(40)</sup>等案件中，欧盟法院又采取了类似立场，将个人信息理解为保护隐私权益的工具。在欧盟法院看来，并不存在一种私法上的个人信息权。在私法上，只有当行为侵犯了具有人格利益的隐私权益时，才能被判定为侵犯个人信息，相关信息主体才有可能得到法律救济。

### 三、法律原理的重新理解

#### (一) 隐私权益的侵权法保护

现代信息社会中，传统的隐私侵权法很难担负起保护隐私权益的重任。例如，有学者指出，英美的隐私侵权法已经停滞不前，在保护个人隐私权益方面捉襟见肘。戴安娜·齐默曼认为，对于普罗斯所归纳的公开个人隐私事实之诉，原告往往很难获胜。<sup>(41)</sup>詹姆斯·惠特曼认为，一个多世纪以来，沃伦与布兰代斯所发展起来的隐私之诉在美国的法律实践中没有多大进展，这一点人们早有共识。<sup>(42)</sup>劳伦斯·弗里德曼更是直言，“沃伦与布兰代斯的隐私观念——防止媒体令人不齿的烦扰——似乎并没有获得多大发展；如今，它基本已经消亡”。<sup>(43)</sup>

传统侵权法难以回应隐私权益在信息与网络时代面临的威胁，原因在于，现代信息社会中，侵犯隐私权益的过程具有复杂性。传统的隐私侵权中，侵犯隐私权益的主体往往是单一或特定的，侵权过程相对容易辨识。侵权法的适用以存在伤害或损失为前提，较为适合对独立的、一次性的侵权提供救济。到了现代信息社会，隐私权益所面临的威胁与风险通常涉及多个主体，侵权过程也不易辨识。例如，个人可能只在小范围内公开了其个人信息，某家企业通过正常的商业活动获取该个人信息后，对这些信息进行了部分匿名化处理，处理后的信息又被转卖给第三方，第三方根据这些信息对用户进行有针对性的电话或网络营销。如同丹尼尔·索洛夫所言，现代社会里，个人隐私权益所面临的威胁具有复杂性、系统性，个人在管理隐私时，往往面临卡夫卡式的困境，很难对伴之而来的相关风险进行分析和判断。<sup>(44)</sup>

要应对这种具有系统性、复杂性的隐私风险，大陆法系的人格权保护进路也存在困难。人格权保护进路将隐私权益视作人格权的一部分，但很多的信息收集、储存、使用与披露行为并不直接对个人人格或其他相关权益造成侵害。尤其是，收集个人信息、使用个人信息、储存与转移个人信息等行为，从单一行为的角度看，可能并不会侵害个人的人格或其

(38) Case C-275/06 Promusicae [2008] ECR I-271.

(39) Case C-73/07 Tietosuojavaltuutettu v. Satakunnan Markkinapörssi OY, Satamedia [2008] ECR I-09831.

(40) Case C-28/08 European Commission v. Bavarian Lager [2010] ECR I-6055.

(41) See Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis' s Privacy Tort*, 68 Cornell L. Rev. 291, 362 (1983).

(42) See James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L. J. 1151, 1204 (2004).

(43) Lawrence M. Friedman, *Name Robbers: Privacy, Blackmail, and Assorted Matters in Legal History*, 30 Hofstra L. Rev. 1093, 1125 (2002).

(44) See Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, New York: New York University Press, 2006, pp. 47-55.

他权益，只有将这些行为集合到一起后，才会对个人人格或其他相关权益造成损害。因此，与英美侵权法的状况类似，<sup>(45)</sup> 大陆法系的侵权法进路也很难为隐私权益提供充分的保护。

## (二) 个人信息的财产法保护

保护隐私权益的另一种私法进路，是将个人信息“权利化”，设想一种对抗不特定第三人的个人信息自决权或财产权。这种个人信息私法保护的进路可能面临隐私权益保护过度与保护不足的双重问题。

一方面，如果赋予个人信息主体以对抗不特定第三人的财产权或自决权，那就意味着，一切获得他人个人信息的行为都必须征得对方的同意，未经他人同意，一切获取他人信息的行为都属违法。在现实社会中，此类情形显然是荒谬的。按照这一逻辑，当前社会中普遍存在的私人信息交流和“八卦”现象都将构成对信息自决权的侵犯。<sup>(46)</sup> 个人信息权或信息自决权的创设，不仅可能会对人们交流第三方信息造成困难，而且会给其他日常交往制造难题。人们在日常生活的交流过程中，经常会涉及到他人信息。这种关涉他人信息的交流通常不可能经过当事人的明确同意，特别是当涉及到他人的负面信息时，当事人往往不会同意他人获知自身的信息。如果赋予个人以完整的个人信息权或信息自决权，必将导致个人信息侵权现象在日常生活中的泛化。<sup>(47)</sup> 总之，如果将个人信息视为一种可以对抗他人的权利，每个人都将成为一座孤岛，既无法进行正常的社会交往，也无法有效获取社会信息。<sup>(48)</sup>

另一方面，将个人信息权利化或财产化，由个人通过企业的“告知—选择”框架保护公民的隐私权益，又会造成公民隐私权益保护不足的问题。<sup>(49)</sup>

个人往往缺乏隐私权益保护意识。在现实生活中，人们不阅读或几乎不阅读相关的隐私公告。在2006年的一项研究中，美国研究者发现，只有20%的被调查者在“大多数情况下会阅读隐私公告”。<sup>(50)</sup> 在另一项研究中，只有4.5%的被调查者表示他们总是阅读隐私公告，14.1%的被调查者称他们经常阅读隐私公告。<sup>(51)</sup> 这在一定程度上说明，格式化的隐私条款或隐私公告在加强个人隐私权益保护方面可能并无明显作用。<sup>(52)</sup> 人们之所以不阅读隐

(45) 有关美国侵权法路径在保护隐私权益方面的不足，参见 Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U. C. Davis L. Rev. 379, 406-408 (2003)。

(46) 对于这种流言、信息流通与科技发展的分析，参见 Daniel J. Solove, *The Future of Reputation: Gossip, Rumor, and Privacy in the Internet*, New Haven, CT: Yale University Press, 2007。

(47) 参见前引〔32〕，杨芳文，第30页。

(48) 就这一点而言，2017年通过的民法总则是具有智慧的。第110条中明确规定了自然人的隐私权，而对于个人信息，则仅仅是在第111条中写入了“自然人的个人信息受法律保护”，并未将此明确定义为一种可以对抗不特定第三人的个人信息自决权。未来对于民法总则的解释有必要继承这一智慧，避免以泛化的私法权利思维来解释第111条。参见王利明主编《中华人民共和国民法总则详解》，中国法制出版社2017年版，第465页。

(49) 对于个人信息财产权的主张者而言，这一结论看上去是违反逻辑和直觉的。在他们看来，从侵权责任转换到财产责任，实际上赋予了当事人以更多“自决权”或谈判的权利，从逻辑上讲，应当可以更好地保护隐私权益。然而，个人信息财产权主张者的乐观预期要想实现，必须满足一个前提条件：个人对于隐私的自我管理能够有效的进行。See Lawrence Lessig, *Privacy as Property*, 69 Social Research 247 (2002)。

(50) Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009, p. 105.

(51) 有的学者甚至认为，格式化的隐私条款或隐私公告对于个人来说几乎都是“形同虚设”。See George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. Interactive Marketing 15, 20-21 (2004)。

(52) See Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. Pa. L. Rev. 647, 671 (2011)。

私公告，原因有多个方面。首先，个体对于风险的认知往往是有限理性的。行为法律经济学的研究者们发现，个人通常对于熟悉的风险，诸如刑事犯罪、疾病等风险感知程度较深，对于不熟悉的风险，如隐私权益保护不力所造成的风险，则感知较浅。<sup>(53)</sup> 因此，个人在面对隐私条款或相关告知时，态度时常是漫不经心的，难以做出真正理性和深思熟虑的选择。<sup>(54)</sup> 其次，隐私保护问题带有一定程度的专业性，非专业人士即使阅读了相关隐私政策，也不可能完全理解政策内容。许多企业和网站的隐私政策十分复杂，远远超出一般读者的阅读能力。不仅如此，这些隐私政策还极为冗长，内容各不相同。以 Facebook 隐私政策的解释为例，其篇幅之长甚至超过美国宪法。<sup>(55)</sup> 公民个体要想完全理解隐私政策，几乎是不可能的。根据卡内基梅隆的一项研究估算，一位美国公民，要想阅读完其访问的所有网站的隐私公告，一年可能需要花费 244 个小时。<sup>(56)</sup>

当然，隐私的自我管理可以通过改善企业和网站的隐私政策部分实现。<sup>(57)</sup> 国家可以要求企业出台清晰易懂的隐私政策，以便个人能够准确无误地理解它们。就像《一般数据保护条例》所规定的，隐私政策“应当使用一种容易理解的形式，使用清晰和平白的语言”。<sup>(58)</sup> 即便如此，现代社会中隐私与风险的特征也无法改变。现代社会中，个人信息的收集、储存、分析、披露等过程已经变得极为复杂，隐私与风险的关系并非一一对应。即便网站提供了清晰的风险预警，个体具有极高的风险意识，人们也不可能合理预见与隐私权益相伴而生的种种风险。

#### 四、隐私权益的场景化与社群主义理解

个人信息的私法保护进路之所以存在困境，根本上是由隐私权益与个人信息的特征决定的。首先，隐私权益总是场景化的，脱离特定场景谈论隐私权益，容易导致隐私权益保护的目的是与效果发生错位。传统的隐私侵权法中，法律制度所要防控和应对的主要是传统类型的侵权行为；而在以公法规制为主的信息与数据保护立法中，法律制度所要防范和化解的主要是计算机与网络技术带来的风险。脱离具体场景谈论隐私权益或个人信息权益，不但无法为权益提供有效保护，还有可能引发过度保护或保护不足的弊端。其次，隐私权益总是同特定社群或特定共同体相联系，在设定隐私权益的保护限度时，必须参考特定共同体的一般标准。尽管隐私权益保护的表现形式是防御第三人或共同体对私人空间的介入，

(53) See Richard H. Thaler & Cass R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness*, New Haven, CT: Yale University Press, 2008, p. 9.

(54) See Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?* in *Digital Privacy: Theory, Technologies and Practices*, Acquisti, De Capitani di Vimercati, Gritzalis, Lambrinouidakis (eds.), Auerbach Publications, 2007, p. 363.

(55) See Bianca Bosker, *Facebook Privacy Policy Explained: It's Longer than the Constitution*, Huffington Post, Apr. 8, 2014.

(56) See Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. Telecomm. & High Tech. L. 273, 274 (2012).

(57) 学者对于改善隐私政策的建议很多，有学者主张必须将企业的隐私政策和企业商标进行捆绑，也有学者主张应当要求企业的隐私政策变得极具警示性，采取类似香烟广告上的警示。See Paul Ohm, *Branding Privacy*, 97 Minn. L. Rev. 907 (2013); M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027, 1050-55 (2012).

(58) 《一般数据保护条例》(679号条例)，第7条第2段。

其目的却在于促进个体在共同体中更好地交流信息，而非使其脱离社会，化为信息孤岛。因此，个体隐私权益受保护的力度必然因其所处共同体的不同而有差异。隐私权益保护的边界，需要根据不同共同体的特点和具体场景中人们的普遍预期加以确定。例如，亲密的小共同体中，对于隐私权益的保护力度往往较小，因为在这样的小共同体中，成员之间对于隐私的相互分享有着较高的接受度。在半熟人社会或陌生人社会中，成员会对隐私与信息的分享较为警惕。在陌生人社会里，人们对隐私保护的预期可能更高，甚至期望彻底实现信息的匿名化，达到人们相互之间无法直接辨识彼此身份的程度。<sup>(59)</sup>

在法律实践中，这种基于场景与共同体的视角已经得到充分体现。20世纪70年代以来，合理信息实践原则已被美国和欧洲的个人信息保护立法广泛采用。从美国的各个部门立法到欧洲最新的《一般数据保护条例》，<sup>(60)</sup>无一例外。尽管合理信息实践原则有多个版本，但它们都假设了市场共同体或政治共同体的存在，假设了信息流通对于市场运转或国家治理的重要性。合理信息实践原则关注的核心问题在于，企业或国家在信息收集与使用的过程中是否贯彻了合理性原则。合理信息实践原则所要求的告知义务、公开义务、透明义务以及赋予当事人更多的知情权和修改权，本质上都是希望信息流通更加符合个体在具体场景中的预期。

在理论界，这种隐私权益的场景化理解与共同体视角也日渐成为主流。1989年，罗伯特·波斯特发表了《隐私的社会基础：普通法侵权中的共同体与自我》一文。<sup>(61)</sup>波斯特指出，隐私侵权法看似是个人防御集体对个体空间或个人人格加以侵犯的手段，实则带有社群主义的面相，因为只有社群共同体中，个人的合理空间或人格才具有实现的可能。普通法上的隐私侵权确定了个人隐私的边界，其所做的无非是保护“社会规范”，即建构个人和共同体身份的“文明规则”。隐私法的功能在于，保护共同体的“社会规范”或“文明规则”不被以媒体为代表的机构所吞噬。海伦·尼森鲍姆所做的研究同样具有奠基性。不同于从个人权利角度看待隐私的研究，尼森鲍姆将隐私问题放置在具体的信息流通场景下加以理解。<sup>(62)</sup>在尼森鲍姆看来，隐私之所以构成现代社会中的重大问题，原因在于现代科技的兴起极大地改变了信息的流通方式，而这种流通方式未必是公平和合理的。隐私保护的合理路径并非是划定一条固定的隐私权或个人信息权的边界，相反，隐私保护所要做的，

(59) 当然，在大数据时代，这一预期或目标能否实现以及在何种程度上实现，是一个复杂的问题。有学者认为，这一预期或目标无法实现，因为在大数据时代，通过各种信息的交叉比对，辨识个人信息已经非常容易，即使通过各种匿名化的技术处理数据，也不足以防止人们通过相关信息识别个人。有学者区分了已识别的个人信息和可识别的个人信息，认为应当将前者视为信息隐私法保护的首要对象，而对后者则应采取不同级别的保护。两种观点分别参见 Paul Ohm, *Broken Promises of Privacy*, 57 UCLA L. Rev. 1701 (2010); Paul M. Schwartz & Daniel J. Solove, *The PII Problem, Privacy and a New Concept of Personally Identifiable Information*, 86 N. Y. U. L. Rev. 1814 (2011)。

(60) 对比美国和德国，会发现美国对于“场景”要更为尊重，美国的《消费者隐私权利法案》直接将“尊重场景”视为核心原则。必须注意的是，尽管欧洲《一般数据保护条例》总体上采取了一种强化数据主体控制的进路，其条文也体现了场景化期待的思路。例如，《一般数据保护条例》第6条第4段规定，当数据主体没有明确表示同意，判断数据处理是否合法，应当考虑“个人数据收集时的目的与计划进一步处理的目的之间的所有关联性”，“个人数据收集时的场景，特别是数据主体与控制者之间的关系”。对于美欧在此问题上的区别，可参见范为《大数据时代个人信息保护的路径重构》，《环球法律评论》2016年第5期，第95页以下。

(61) See Robert C. Post, *The Social Foundations of Privacy: Community and the Self in the Common Law Tort*, 77 Cal. L. Rev. 957-998 (1989)。

(62) 参见前引〔50〕，Nissenbaum文，第67页以下。

应是实现“场景性公正”，即在具体场景中实现信息的合理流通。经过波斯特、尼森鲍姆等人的奠基性研究，如今的隐私研究尽管仍然众说纷纭，场景化和共同体的分析思路，却已为越来越多的学者所接受。例如，有学者从信任的角度分析隐私，认为隐私的本质是一种信任，即一方合理地信任另一方或者相关方不会泄露其信息；<sup>(63)</sup> 有学者认为，可以借助英国普通法上的违反保密之诉重新激发隐私侵权法的活力。<sup>(64)</sup> 这些研究的共同之处在于，都将隐私权益保护置于共同体或某种关系网中加以思考，并结合具体场景，判断侵犯隐私权益的情形是否存在。<sup>(65)</sup>

## 五、迈向个人信息的消费者法与公法保护

同西方国家一样，我国个人信息的私法保护也面临着许多困境。一方面，随着互联网、大数据与信息技术的发展，当前民法体系中的隐私权保护机制难以应对现代信息社会中的新挑战，传统侵权法无法适应现代信息社会中的复杂风险。另一方面，过度依赖私法中的意思自治原则或“告知—选择”框架来保护个人信息，会给个人和企业制造难题。对于个人而言，由于隐私政策专业性太强、个人认知有限、信息风险复杂等原因，个人难以对自身的隐私权益和其他权益进行准确判断。对于企业和其他机构而言，如果要求个人信息的使用都要以明确授权为基础，那么社会中的个人信息流通就会面临巨大阻力。企业和相关机构对个人信息的合理收集与利用就会面临许多障碍，进而损及社会公共利益和公民的其他权益。

为摆脱个人信息私法保护的困境，我国的个人信息法律保护应当倚重消费者法保护与公法保护的进路。为真正发挥私法在保护公民隐私权益方面的作用，国家有必要结合具体场景，将私法“消费者法化”。个人信息法律保护的背景是，现代信息社会中个体与企业等大型机构之间在信息能力方面存在巨大差异，这与强调主体平等、意思自治的私法存在隔阂。私法若要在保障个人信息的合理流通与使用的同时，兼顾对公民隐私权益的保护，就必须结合具体场景，采用以倾斜保护、集体保护等为原则的消费者法框架。在个人信息消费者法保护的具体制度层面，我国未来的个人信息立法可以在特定领域和特定情形中赋予个体以具体的消费者权利，如个人信息访问权、纠正权等。通过在特定场景中进行赋权与倾斜保护，而非一般性的赋权，公民个体将能对自身信息与相关权益进行有效的自我保护，企业、政府机构和社会也能实现对个人信息的合理利用。同时，各级消费者权益保护委员会可以针对企业在个人信息保护方面的一些不当行为提起公益诉讼，检察机关也可对此开展公益诉讼的探索。单一个体或消费者很难对企业等信息收集者与处理者进行监督，但各类公益组织和政府机构可以成为消费者集体或公民集体的代言人，对个人信息保护进行有效监督。

(63) See Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. Miami L. Rev. 559 (2015).

(64) 参见前引〔41〕，Zimmerman文。

(65) 正如有的学者所言，分析隐私必须将隐私放在“信息共享的场景下，用社会学的人际信任的原则，而不是基于权利教义的自主和选择框架”。参见前引〔63〕，Waldman文，第560页以下。国内研究中类似的观点，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，第84页以下。

公法保护也应当成为我国个人信息保护的重要手段。之所以要保护个人信息,很大程度上是因为个人信息的保护不足或保护不当会给公民个体带来无法预见或无法预防的风险。如果国家能够对相关风险进行有效预防与管理,个体防范相关风险的压力就会降低很多,个人信息的收集、使用和流通也能较为安全。在公民个体不足以对信息风险进行客观和有效判断的情况下,国家有责任为公民提供信息安全这一公共产品。就个人信息公法保护的具体制度而言,我国未来的个人信息立法可以建立一套风险管理制度。例如,针对某些收集、储存与处理个人敏感信息或海量个人信息的网络与信息设备,可以比照网络安全法第31条的规定,要求企业等机构采取严格的安全保护义务。对于一般企业与机构的个人信息收集与利用,可以借鉴和采用风险评估与风险预防制度,实现对相关风险的有效管理。<sup>(66)</sup>

---

---

**Abstract:** Contemporary studies on information privacy adopt an individualistic approach and view personal information as an object of civil right. These studies argue that, according to foreign experience, civil law could provide effective protection to privacy. Yet this article argues that Western information privacy law has never endorsed a civil right to personal information. Meanwhile, traditional civil law faces great difficulty in providing effective protection to citizens' privacy in the age of information society. We should adopt a contextualized understanding of privacy and realize that the flow of personal information is a common good. The aim of protecting personal data is to regulate the risks associate with personal information and to promote the proper flow of personal information in concrete context. Therefore, we should employ consumer protection law to reinvigorate the civil law protection of personal information. Meanwhile, we should also employ public law to regulate risks and protect personal information.

**Key Words:** privacy, personal information, civil law protection, consumer protection, risk regulation

---

---

(66) 类似的立场,参见周汉华《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》,《法学研究》2018年第2期,第3页以下。在域外的个人信息保护中,这一思路也得到了体现。例如,欧洲《一般数据保护条例》第32条规定了与风险相称的技术与组织措施“在考虑了最新水平、实施成本、处理的性质、处理的范围、处理的场景与目的之后,以及处理给自然人权利与自由带来的伤害可能性与严重性之后,控制者和处理者应当采取包括但不限于如下的适当技术与组织措施,以便保证和风险相称的安全水平。”第35条规定了风险评估“当某种类型的处理——特别是适用新技术进行的处理——很可能对自然人的权利与自由带来高风险时,在考虑了处理的性质、范围、场景与目的后,控制者应当在处理之前评估计划的处理进程对个人数据保护的影响。”