从隐私到个人信息:利益再衡量的理论与制度安排

张新宝*

内容提要　传统隐私权保护法主要考虑的是隐私权人与其他人(义务主体)在隐私保护与言论表达自由、知情权实现等方面的利益衡量问题,尽管公共利益是重要的制约因素,但国家尚未以利益主体的身份登场,立法政策倾向于对个人隐私提供"绝对"的保护。在个人信息保护法治中,尽管这组利益关系仍存在,但国家不再单纯以超然利益关系的治理者出现,它同时也是最大的个人信息收集、处理、储存和利用者。更重要的是,信息业者作为独立的主体出现。个人信息保护法需要衡量更多的利益关系。在新的利益衡量格局下,我国的个人信息保护法应以"两头强化,三方平衡"理论为基础,并为实现该理论设计一组相互关联的制度方案。

关键词　个人信息保护　隐私权　利益衡量　"两头强化,三方平衡"

DOI:10.14111/j.cnki.zgfx.2015.03.003

引　言

个人隐私又称私人生活秘密或私生活秘密,是指私人生活安宁不受他人非法干扰,私人信息保密不受他人非法搜集、刺探和公开。隐私包括私生活安宁和私生活秘密两个方面。[①] 个人信息[②]是指与一个身份已经被识别或者身份可以被识别的自然人相关的任何信息,[③]包括个人姓名、住址、出生日期、身份证号码、医疗记录、人事记录、照片等

* 国家社会科学基金2014年重大项目《互联网安全主要问题立法研究》(项目批准号:14ZDC021)首席科学家,中国人民大学法学院教授,本刊总编辑。本文是该项目子课题《个人信息安全保护立法研究》阶段性成果,由张新宝、葛鑫、张乐执笔。子课题成员还有:李长喜(国家互联网信息办公室政策法规局处长)、王旭(中国人民大学法学院副教授)、姜强(最高人民法院民一庭法官)、陈璞(中国人民大学副研究员)、张乐(河南师范大学法学院副教授)、葛鑫(中国人民大学法学院博士研究生)。

① 参见张新宝《隐私权的法律保护》,群众出版社2004年版,第7页。相同观点参见王利明《隐私权概念的再界定》,载《法学家》2012年第1期。

② 也有学者使用个人数据、个人资料、信息隐私等称谓,但研究对象和内容并无本质区别。本文遵从目前学界和实务界共识,采"个人信息"称谓,与"个人数据"意义相同。

③ *See* General Data Protection Regulation, Article 4.

单独或与其他信息对照可以识别特定的个人的信息。④ 个人隐私与个人信息呈交叉关系,即有的个人隐私属于个人信息,而有的个人隐私则不属于个人信息;有的个人信息特别是涉及个人私生活的敏感信息属于个人隐私,但也有一些个人信息因高度公开而不属于隐私。传统隐私法(或保护隐私权的民法制度)将隐私权作为人格权之一种进行保护,所侧重的是个人的人格利益尤其是人格尊严和人格自由方面的利益。人类进入信息社会后,与个人信息相关的利益主体及其利益关系变得多样和复杂,对个人信息采取了保护与利用并重的基本立法政策,信息业者(即从事个人信息收集、处理、储存、传输和利用等相关活动的自然人、法人和其他组织)作为独立的利益相关者出现,国家不再是超然的法律规则制定者和执行者,同时也是个人信息最大的收集、处理、储存和利用者。

对于个人信息保护立法,欧盟采取了"'指令'⑤+成员国立法"的"国家主导模式",美国则采取了"补充已有法律(主要是隐私权保护法律)+行业自律"的模式。国内学者对这一问题的研究已持续10多年,主要成果包括三个方面:一是我国个人信息保护的法律基础理论研究,⑥二是关于个人信息保护法的专家建议稿,⑦三是对个人信息保护的一些具体制度(如网络实名制)的研究。⑧ 从立法进展看,我国也制定了一些规范性文件,对个人信息保护问题进行了原则性和框架性的规定,但尚未构成体系化的个人信息保护法律制度。

本文将观察从隐私保护到个人信息保护的社会和法治变迁过程,讨论个人信息保护与利用关系的各相关主体及其利益关系的变化情况,发掘与表达这些相关主体的主要利益诉求,利用立法利益衡量的原理和方法平衡各方利益,进而提出"两头强化,三方平衡"理论作为个人信息保护与利用法治的基础理论,并探索这一理论在个人信息保护立法中的主要实现路径。

---

④ 参见《中华人民共和国个人信息保护法(专家建议稿)》第9条,转引自周汉华《〈中华人民共和国个人信息保护法(专家建议稿)〉及立法研究报告》,法律出版社2006年版,第3页。

⑤ *See* Directive 95/46/EC(《个人数据保护指令》,2012年11月修订为General Data Protection Regulation《欧盟数据保护规则》)、Directive 2000/31/EC(《电子商务指令》)、Directive 2002/58/EC(《隐私与电子通讯指令》)、Directive 2006/24/EC(《数据留存指令》)。

⑥ 相关研究成果参见齐爱民《个人资料保护法原理及其跨国流通法律问题研究》,武汉大学出版社2004年版;孔令杰《个人资料隐私的法律保护》,武汉大学出版社2009年版;蒋坡《个人数据信息的法律保护》,中国政法大学出版社2008年版;郭瑜《个人数据保护法研究》,中国政法大学出版社2012年版。

⑦ 参见前引④,周汉华书;齐爱民《中华人民共和国个人信息保护法示范法草案(学者建议稿)》,载《河北法学》2005年第6期。

⑧ 参见齐恩平《实名制政策与私权保护的博弈论》,载《法学杂志》2013年第7期;马艳华《网络实名制相关法律问题探析》,载《河北法学》2011年第2期;杨晓楠《网络实名制管理与公民个人信息保护》,载《情报科学》2012年第11期;王秀哲《身份证明与个人信息保护——我国居民身份证法律规制问题研究》,载《河北法学》2010年第5期;王锐、熊健、黄桂琴《完善我国个人信用征信体系的法学思考》,载《中国法学》2002年第4期;孙平《政府巨型数据库时代的公民隐私权保护》,载《法学》2007年第7期。

一、隐私权的法律保护与相关利益衡量

(一)隐私权的法律保护

1. 隐私权被确认为人格权

对隐私的保护需求作为一种人类的自然情感,来源于人类的羞耻本能,[⑨]但将隐私利益上升为一种个人权利与法律相联系则源于 1890 年 Samuel D. Warren 和 Louis D. Brandeis 的《论隐私权》一文。该文作者认为,面对社会生活的发展,普通法应当认可 Thomas Cooley 法官所称的"个人独处权利",[⑩]保护个人有权选择自己的生活,而不受外界的干涉或侵害,除非存在明确的社会需要和合法依据。自此之后的百余年间,隐私权在美国获得了长足发展:在侵权法领域以 William Prosser 所总结的隐私侵害四种类型而呈现体系化;[⑪]为保护隐私不受来自公权力的侵害,美国联邦最高法院认定隐私权是宪法上未列明的基本权利,逐渐形成宪法上自决性隐私和信息性隐私两大领域;为应对个人信息保护与利用问题,美国还通过制定相关保护信息隐私的成文法来加以规范。总之,美国隐私权存在于宪法、侵权法和各类成文法。有美国学者甚至将隐私权比喻为变色龙,"它的含义根据其所在背景和语境的不同而不断变化。"[⑫]

隐私权在美国走过一百多年的历程间,大西洋对岸的欧洲各国也面临着同样的问题。《欧洲人权公约》[⑬]将公民私生活保护列为公民基本权利。在二战后人权保护的大环境下,欧洲各国国内法也陆续制定法律予以回应。在英国,虽然法律对公民的隐私予以保护,但一直不认可侵害隐私可以作为独立诉由,而是将侵害隐私的案件纳入其他侵权行为的范畴,这使得英国的隐私保护不够发达而较为零碎。[⑭] 在德国,隐私是一般人格权萌生和发展的源头,同时经由一般人格权的认可而获得保护。二战后窃听谈话、秘密录音等非法干预他人私生活的行为日渐弥漫,为了给受害人提供救济,宪法法院在"读者来信案"[⑮]中引入"一般人格权"概念。作为一种框架性权利,一般人格权具体化的典型类别便是为个人隐私提供保护的"私领域"。此后,德国宪法法院在"人口普查案"[⑯]中认为个人资料是自然人人格的勾画,"个人得本诸自主决定的价值与尊严,自行决定何时及于何种范围内公开其个人的生活事实"。[⑰] 从而确立"资讯自决权",成为此后德国隐私保护的理论基础。在法国,"早期法国法的观念和此观念支配下的人格保护

---

⑨ *See* CARL D. SCHNELDER, SHAME, EXPOSURE, AND PRIVACY, W. W. Norton & Co Lnc, 1992.

⑩ THOMAS M. COOLEY, LAW OF TORTS, Calllaghan & Company, 2nd ed ,1888, p. 29.

⑪ *See* William L. Prosser, *Privacy*, 48(3) Cal. L. Rev. 383, 389(1960).

⑫ DECKLE MCLEAN, PRIVACY AND ITS INVASION, Praeger Publishers,1995, p3.

⑬ 《欧洲人权公约》第 8 条规定:人人有权享有使自己的私人生活和家庭生活、家庭和通信得到尊重的权利。

⑭ 参见王泽鉴《人格权的具体化及其保护范围:隐私权篇(上)》,载《比较法研究》2008 年第 6 期。

⑮ BGHZ 13,334.

⑯ BVerfGE 65,1.

⑰ 前引⑭,王泽鉴文。

的实践,还没有涉及到自然人的隐私和个人生活等范畴"。[18] 法国对隐私的关注伴随着对新闻自由的限制,体现在宪法上"侮辱或诽谤他人私人生活的"保护措施的规定;19世纪50年代,一些著名的案例确定了"个人形象权"的保护。1970年《法国民法典》修改之时,在第9条规定了"私生活受尊重权"。

2. 隐私利益保护的主要法理

资产阶级革命带来的人文主义和自由主义思想,工业革命和电气革命催生的物质文明,都使得隐私的观念率先在西方社会深入人心,并形成了两种不同的隐私文化。总体上来说,美国从自由的角度理解隐私,而欧洲大陆将隐私保护植根于人格尊严之上。耶鲁大学惠特曼教授也认为两者的隐私制度拥有两种不同的价值核心:"一方面是主要被大众媒体威胁的个人尊严利益,这属于欧洲;另一方面是主要被政府威胁的自由利益,这存在于美国。"[19]

在美国,基于特殊的独立和建国历史,长期以来政治和社会理念主要围绕着对警察和其他政府官员的不信任循环而展开,[20]其隐私观念也就更多地体现在对禁止国家侵扰这一消极自由的追求,许多美国学者以《1984》中老大哥监控下的恐怖集权政府形象,强调隐私保护的的重要性。法律为个人提供隐私保护,个人得以从公共生活和公众视线退出,在日益扩张的公权力之下和日益紧张的社会生活中仍然享有独处的时空,个人可以真实地生活,发展个性而不受他人支配和操纵。"隐私是人类价值的缩影,这些价值可以概括为'个人自决'、'个性'和'个人人格'。"[21]借由隐私权的保护路径,不仅促成了个人的独立自主,也有助于民主社会的维持和国家权力的限制。

欧洲大陆历来有维护人格尊严的传统,只不过早期对人格尊严的维护限于贵族等少部分人。随着人文主义思想的传播,对于人格尊严的保护才逐渐及于每一个社会成员。二战后,对纳粹践踏人类尊严的沉痛反思促使其将人格尊严作为法律体系的核心价值和伦理基础。与美国保护隐私利益的法理相比,欧洲大陆更多地从人格尊严的角度确认对个人私生活的保护的必要。"当我们的隐私被非法地暴露于公众面前时,我们的自尊也被摧残了,我们与他人之间的关系也受到了损害,这就是法律为什么要保护隐私的原因。"[22]

(二)隐私权保护的利益衡量

文明是逐渐迈向拥有隐私权的社会过程。在社会结构、居住环境、技术进步和大众传媒发展使得个人与社会生活之间关系愈加紧张之时,人们日渐产生避免其私生活遭

---

[18] 龙卫球《论自然人人格权及其当代进路——兼论宪法秩序和民法实证主义》,载《清华法学》2002年第2期。

[19] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113(6) Yale Law Journal 1151, 1221 (2004).

[20] *Id* 19.

[21] [美] 阿丽塔·丽·艾伦、理查德·伦、理托克音顿《美国隐私权:学说、判例与立法》,冯建妹等编译,中国民主法制出版社2004年版,第17页。

[22] Ruth Gavison, *Privacy and the limits of Law*, 89 Yale Law Journal 421, 471(1980).

受公开的权利诉求，以对抗大众传媒、公众评论、大众窥私欲对私人生活领域的侵入。经过人文主义和自由主义洗礼，对个体的尊重被提升至前所未有的高度。要满足个人自由和有尊严地生存和生活的需求，就必须认可对个人私生活秘密和私生活安宁的法律保护。由此，隐私权也被塑造为绝对性和对世性的抵御权利。但个人总是社会的一分子，纯粹的离群独处并不现实，法律还保护个体知悉、获取信息的自由以及表达自我思想的自由，法律为个人隐私提供保护也就意味着对他人此等自由的限制。这就体现为隐私权与知情权和言论自由的利益冲突。

知情权是个人对公共事务及与自己有关或感兴趣的事务接近和了解的权利，包括知政权、社会知情权和个人信息知情权。[23] 个人一方面不希望自己的私生活被他人知悉或干涉，同时又渴求自己可以获得和知悉尽可能多的信息以满足其政治和精神需求。隐私旨在保护个人从公共生活和公众视线中退出的自由，其所涉及的是与社会公共利益和群体利益无关的私人生活，“公共领域和私人领域之间的区分是构建隐私权法的核心”。[24] 当知情权的内容涉及到社会公共利益或者公众的合理兴趣时，法律认可此种社会公共利益相较于个体隐私利益的优越性，公众的知政权和社会知情权分别构成了对国家官员隐私权和社会公众人物隐私权的限制。隐私权和个人信息知情权之间的冲突多发生在具有某种事实上或者法律上特别关系的个体之间：一方个人信息知情权所要了解的对象正是另一方隐私权所要保护的对象。此时法律通过权利协调原则，认可个人了解与其自身有关的事务的权利的正当性，但同时要求个人信息知情权人不得再行披露他方当事人的隐私，以保护隐私权人。

言论自由也称言论和表达自由或表达自由，指公民有权以语言或者其他任何方式表达思想，其核心为“人人有主张及发表自由之权。”[25]同时，作为实现表达自由的途径，法律还必须确保个人获取和传播信息的自由，言论自由和知情权相互依赖、相互促进。法律对言论自由的保障，不仅适用于为社会普遍接受的无涉价值判断的言论，也适用于一些能够使人不愉快、扰乱国家或者不利于某一群体的言论。“对信息隐私的保护不能侵害言论自由、妨碍具有新闻价值和公共关注的问题的信息的传播。”[26]言论自由与隐私权之间便不可避免地产生了冲突。通常说来，当言论涉及到社会公共利益、社会公众的合理兴趣时，言论自由构成隐私权侵权的合理抗辩；当言论仅仅涉及个人私生活而无涉公共生活时，对于二者冲突的协调则取决于法律的态度，如美国历来重视言论自由对民主的价值，法律实践中认为原告必须证明被告对其言论存在“真实恶意”才能构成对隐私权的侵犯，由此对隐私权给予更多的限制。

---

[23] 参见前引①，张新宝书，第 85-87 页。

[24] RICHARD C. TURKINGTON & ANITA L. ALLEN, PRIVACY, 2nd ed., West Group, 2002, p. 1.

[25] 《世界人权宣言》第 19 条“人人有权享有主张和发表意见的自由；此项权利包括持有主张而不受干涉的自由，和通过人任何媒介和不论国界寻求、接受和传递消息和思想的自由。”

[26] Matthew C. Keck, Cookies, *The Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet*, 13 (1) Albany Law Journal of Science & Technology 83, 117(2002).

隐私权、知情权与言论自由同是个人享有的基本权利和自由,都为维持个体的人格尊严和自由、增进民主社会的多元化所必须,面对不同个体在基本权利和自由之上的冲突,国家作为超然于个体权利冲突之外的中立第三方,以立法和司法裁判的方式进行利益冲突的协调。一方面,隐私权逐渐上升为一项绝对性和对世性人格权的过程意味着其得到了以法律形式体现的国家意志的认可;而与此同时,为协调隐私权与知情权、言论自由之间的冲突,法律同样认可社会公共利益构成对个人隐私权的合理限制,当知情权、言论自由符合社会公共利益旨趣时,新闻价值、公共人物等限制构成对隐私权侵权的有效抗辩。

在隐私权制度设计时,主要需要平衡的只有一对利益矛盾,即隐私权主体(个人)的隐私利益(也可以表达为人格自由与人格尊严方面的人格利益)与他人(即负有消极不作为义务的其他自然人、法人或者其他组织)的言论表达自由、知情权等利益的冲突。国家基本上处于一个超然于双方利益矛盾的中立地位,以社会管理者身份,通过制定法律和实施法律调整矛盾双方的利益关系。国家调整这一利益关系的主要手段就是"公共利益"规则的适用:凡不涉及公共利益的个人隐私,受到保护;凡涉及公共利益的隐私,或者不予保护,或者受到限制。

二、个人信息的法律保护及相关利益衡量

(一)个人信息的法律保护

随着个人信息处理方式的数字化转变,人们在享受信息数字化带来的诸多便利的同时,也面临着个人信息数字化带来的风险。近半个世纪以来,有关个人信息保护的立法已经成为全球范围内最为瞩目的立法运动之一。到目前为止,全球已经有 90 多个国家制定了个人信息保护法。在应对现代化方式进行个人信息收集和利用行为时,欧洲大陆国家进行了专门性立法的尝试,对个人信息的收集和利用行为加以规范,以弥补其隐私保护的不足。1970 年德国黑森州制定的《黑森州数据法》是世界上第一部专门性个人数据保护法;1973 年的《瑞典数据法》是世界上首部全国性的个人数据保护法;1977 年德国也制定了全国性的《联邦数据保护法》;1978 年法国通过了《信息、档案与自由法》;1984 年英国在争议中通过了《英国数据保护法》。这些国家的个人数据保护立法对后来整个欧洲的数据保护产生了广泛而深远的影响。1995 年欧盟通过《个人数据保护指令》,也采取了个人数据保护统一立法模式。[27] 在欧盟的强大实力影响下,该指令对于全球范围内的个人信息保护立法都有实质影响。

而美国在其隐私保护较为完善的法律体系之下,对个人信息保护问题,最初是通过"信息控制权"理论修正其隐私权概念,为个人对其信息的积极控制提供支持。"水门事件"的曝光,触动了美国社会对于警察政府的敏感神经,催生了 1974 年《隐私法案》。

[27] *See* Directive 95/46/EC, Article 3.

该法强调联邦政府对个人信息收集和利用的公平性和正当性，也促使联邦政府为公民个人信息提供积极保护，避免不当披露或滥用侵害个人隐私。在私人领域，出于对市场调节的信奉和支持信息技术发展的考虑，美国采取了“零售式”分散立法模式，针对特定行业或领域内的个人信息收集和利用问题单独立法。[28]

伴随着信息化进程的推进，我国法律对个人信息保护与利用问题也作出了回应。2000 年 12 月 28 日，全国人大常委会《关于维护互联网安全的决定》是我国以法律规范互联网的开端，该决定将信息安全视为互联网安全的重要内容，采取刑事制裁手段维护信息主体权利，其中第 4 条规定“非法截获、篡改、删除他人电子邮件或者其他数据资料，侵犯公民通信自由和通信秘密”可构成犯罪；2012 年 12 月 28 日，全国人大常委会通过《关于加强网络信息保护的决定》，其中第 1 条明确规定“国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息”，并遵从国际惯例规定了多项个人信息保护和利用的基本原则。在部门法方面，2005 年 2 月 28 日，全国人大常委会通过《刑法修正案（五）》，新增“窃取、收买、非法提供信用卡信息罪”；2009 年 2 月 28 日，全国人大常委会通过《刑法修正案（七）》，新增“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”；2009 年 12 月 26 日颁布的《侵权责任法》规定了对隐私权的保护及网络侵权责任；2013 年 10 月 25 日修订的《消费者权益保护法》也对消费者个人信息保护给予重视。[29] 在行政法规和部门规章方面，以国务院 2013 年 1 月 21 日发布的经过修订的《征信管理条例》最为完善，对征信行业的个人信息采集进行了详细规定；工信部作为我国信息产业主管部门，也制定了许多规范性文件，其中以 2013 年 7 月 16 日发布的《电信和互联网用户个人信息保护规定》最具针对性，规定了电信业务经营者、互联网信息服务提供者的个人信息收集、使用规范和安全保障措施。2013 年 2 月 1 日起，国家质量监督检验检疫总局、国家标准化管理委员会联合发布的《信息安全技术-公用及商用服务信息系统个人信息保护指南》（以下简称“《个人信息保护指南》”）开始实施，这是我国首个个人信息保护国家标准。此外，2013 年 9 月 5 日，最高人民法院、最高人民检察院发布《关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》，对通过网络散布捏造损害他人名誉的事实的行为，将信息网络上涉及他人的原始信息内容篡改为损害他人名誉的事实并加以散布的行为认定为“捏造事实诽谤他人”；2014 年 6 月 23 日，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 条对利用网络公开他人个人信息行为的侵权责任认定加以规定。尽管有如此多的规范性文件涉及到个人信息保护，但从整体来看，我国有关个人信息保护的立法尚存在以下问题：一是立法的碎片化现象突出，系统的专门立法尚付阙如；二是对个人信息保护的利益衡量不清晰，表达不准确；三是多数规范性文件位阶偏低，高位阶的

---

[28] 如 1970 年《正当信用报告法》、1978 年《金融隐私权法》、1984 年《有限电视通信政策法》、1988 年《录影带隐私权保护法》、1991 年《电话购物消费者保护法》、1994 年《驾驶员隐私保护法》、1998 年《儿童网上隐私保护法》、1999 年《金融服务现代化法》、2003 年《反垃圾邮件法》等。

[29] 参见《中华人民共和国消费者权益保护法》第 14、29、50、56 条。

规范性文件流于形式或者宣示性规定,缺乏可操作的具体规则;四是相关行政执法部门的定位、权限等不明确,国家互联网信息办公室的行政管理和执法活动缺乏必要的法律依据。

(二)个人信息保护与利用的利益衡量

20 世纪中叶以来,以微电子、电子通讯和计算机等技术为核心的信息技术浪潮引发了新一轮技术革命,推动人类逐渐迈进信息社会。随着社会信息化进程的推进,信息以前所未有的速度和广度被开发利用,信息成为和物质、能量同样重要的资源,整个社会对于信息的依赖和利用需求增强;个人信息的利用在增进社会福祉的同时,也可能引起信息主体的权益受到威胁和侵害,由此催生了个人信息保护的需要。这样的需要体现着各方主体的利益。面对多元化和冲突化的各种利益,法律是在无限需求和有限资源之间寻求平衡的最佳机制,通过立法利益衡量实现对不同利益上下位阶的合理安排。

1. 个人信息价值分析

(1)人格尊严和自由价值

个人信息是"可以识别个人身份的信息",作为个人人身、行为状态的数据化表示,是个人自然痕迹和社会痕迹的记录。个人信息指向信息主体,能够显现个人的生活轨迹,勾勒出个人人格形象,作为信息主体人格的外在标志,形成个人"信息化形象"。在信息社会,人们也已经习惯以个人信息化形象指代真实个人。在现代信息技术之下,几乎所有的个人行为都会留有信息痕迹,这些信息痕迹关涉个人生活的方方面面,实现了对个人从摇篮到坟墓的全程记录;现代化信息技术也可以实现对个人碎片化信息的整合,随着信息质和量的累积,碎片化的个人信息逐渐形成个人的"人格剖面图"。马斯洛在其需要层次理论中指出,"人格标识的完整性与真实性是主体受到他人尊重的基本条件"。[30] 个人作为目的性的存在,只有消除个人对"信息化形象"被他人操控的疑虑和恐慌,保持其信息化人格与其自身的一致性而不被扭曲,才能有自尊并受到他人尊重地生存与生活。因此,个人信息对于信息主体的人格尊严和自由价值,应当是个人信息保护立法中首要考虑的因素。

(2)商业价值

个人信息商业价值的发掘与商业运作尤其是营销模式的改变有重大关联。营销建立在对消费者需求的准确把握之上。从早期大规模营销到定向营销、数据库营销的转变,伴随着经营者收集和利用消费者个人信息能力的提高:计算机、互联网和互动式数字媒体的推广普及,大大拓展了经营者获取消费者信息的渠道和范围,精确了解消费者需求和偏好成为可能,经营者可以更高效地发布广告,享受营销回应比率提升带来的经济回报。信息技术的进一步发展,使得商务智能分析成为现实,而将商务智能技术应用于经营者所掌握的消费者信息,帮助经营者以消费者整体需求为导向,进行未来产品和服务升级更新,大大提高了其决策的效率和理性,实现消费者和经营者之间"有的放矢"的互动。

---

[30] [美]亚伯拉罕·马斯洛《动机与人格》,许金声译,中国人民大学出版社 2007 年版,第 31 页。

个人信息对于整个商业环境的健康运行也至关重要。市场经济是信用经济，社会再生产过程的全部联系都以信用为基础，信用已经成为维护市场秩序和经济发展的关键要素。在信用经济的大背景之下，建立健全完善的社会信用体系关系到整个社会的经济运行，而这显然离不开全国甚至全球范围内大规模的个人信用信息的收集、处理和利用等活动。

公私机构对个人信息的广泛需求还催生了专门的个人信息服务提供者，后者通过大量收集个人信息，形成各种类型的个人信息库，对外提供查询或租赁乃至销售等信息服务，如电话黄页服务、私营征信机构、信贷咨询公司、信息查询平台等。同时，其他信息服务的提供也都离不开个人信息的收集和处理。

伴随着整个社会信息化进程的发展，信息资源成为重要生产要素、无形资产和社会财富，信息化与经济全球化相互交织，推动着全球产业分工深化和经济结构调整，重塑着全球经济竞争格局。[31] 我国作为信息化的后起国家，在赶超世界信息化进程时，不论是传统产业信息化改造、传统服务业转型和信息服务业的发展都需要从整体上提高信息资源的开发利用水平，促进个人信息的开发利用当属应有之义。

(3) 公共管理价值

正所谓“欲得民必先知民”。为实施社会管理和提供公共服务，收集和利用个人信息，是自古以来政府都普遍采用的做法。人口普查作为各国政府各个时期获取人口资料、掌握国情国力最基本的调查方法，已经有几千年的历史。[32] 信息社会中，借助于现代信息技术，政府可以更加充分地发掘个人信息的公共管理价值。信息技术与统计学、数据分析技术的结合，政府可以低成本地收集和存储更多的个人信息，为确定社情民意提供更广泛的分析样本；通过对个人信息的处理和利用，政府也可以实现科学和理性决策，更好地推进公共管理和公共服务。“数字政府”在“责任政府”和“服务政府”的基础上已经成为现代政府的基本标志。[33] 公共秩序、公共安全和公共福利的推进，都离不开以个人信息为基本单位的数据库的支撑。

9·11 事件之后，反对恐怖主义、维护国家安全成为国际主流。恐怖主义被视为 21 世纪威胁人类生存的主要敌对力量。全球反恐形势日益严峻，反恐逐渐常态化，与犯罪相关的个人信息对于提高政府执法效率、有效打击犯罪与保障人权来说是重要的社会管理资源力量。美国国家安全局通过电话监控记录得知本·拉登的踪迹，最终成功将其击毙。2011 年英国伦敦地铁骚乱案中，英国警方也是通过分析留存的通讯数据，才能迅速抓捕与骚乱有关的恐怖分子，平复社会恐慌。如今，在政治目的的裹挟之下，恐怖主义犯罪日渐疯狂和极端，已成为国际社会的巨大隐患，而个人信息对于政府线索溯源和情报分析的价值，必将助力全球恐怖主义活动的预防和侦查，有助于整个国际社会的稳定。

---

[31] 参见中共中央办公厅、国务院办公厅《2006-2020 国家信息化发展战略》，载 http://www.gov.cn/test/2009-09/24/content_1425447.htm，最后访问时间：2015 年 4 月 30 日。

[32] 参见鲁礼新《人口与环境简论》，黄河水利出版社 2010 年版，第 54 页。

[33] 参见蒋坡《公共管理事务中个人数据信息保护的法律问题研究》，载陈海帆、赵国强主编《个人资料的法律保护 放眼中国内地、香港、澳门及台湾》，社会科学文献出版社 2014 年版，第 139 页。

推行电子政务一直是我国信息化发展的战略重点。自上世纪70年代以来,我国就开始探索计算机在国民经济、人口、社会等方面的统计应用。2002年,我国将国家人口基础信息数据库列为国家电子政务重点建设的四库[34]之一。十多年来,我国政府数据库建设工作卓有成效,以公安部所掌握的个人信息数据库类型为最多,包括人口信息管理系统、出入境/证件信息数据库、全国违法犯罪中心、DNA数据库等;另外,国家统计、社会保障、税务等多个管理部门也建立了相应的个人信息数据库。2004年起,我国着手推动人口基础信息共享工作,整合政府部门的人口信息资源,以公安部门的人口信息为基础,逐步融合计划生育、统计、民政、社会保障、税务、教育等部门的信息资源。《2014联合国电子政务调查报告》显示,我国的电子政务发展在全球排名第70位,[35]处于中等水平。而进一步推动我国数字政府建设,必然离不开对个人信息资源的充分正当利用。

2. 个人信息保护与利用的利益识别

"立法是认识利益、表达利益的过程。要调整好各种不同的利益,首先要了解和认识利益。"[36]利益衡量以利益识别为起点,围绕着"个人信息资源"的保护与利用存在如下主要的利益需求:

(1)信息主体对个人信息的保护需求

个人信息承载信息主体的人格利益,本诸于人的自由与尊严,信息主体要求法律对其此种人格利益予以保护,而不能以纯粹物质化的思维来看待个人信息。一方面,其他个体对侵害私人生活秘密的可能性仍然存在(这与隐私保护所面临的问题是相同的),并且因为网络环境的虚拟性和网络传播的便捷和广泛性,个人的隐私保护需求更加强烈;另一方面,现代信息处理技术之下,个人信息所蕴含的公共管理价值和商业价值,将成为公私机构不当收集、处理、利用和传输个人信息的巨大诱因。并且,此种信息不限于传统隐私权之下的私人生活秘密,而且及于个人所有具有可识别性的信息。相较于传统隐私权个人个体化的隐私保护诉求而言,个人对其个人信息的保护诉求更为强烈和普遍,并且已经上升为普遍的社会问题。

信息社会的显著标志是社会从有形的物质创造价值转向无形的信息创造价值,整个社会对于信息资源的依赖性加强,处于社会信息化进程中的个人也概莫能外。在日常生活中,个人无时不刻不在利用公私机构提供的相关信息服务:最为普遍的搜索引擎服务实际上就是一个巨大的互联网信息检索和查询系统,其有效运转必然依赖于大量关涉个人的信息收集和处理;各种身份核查服务、信用咨询服务本身就是整个社会层面个人信息利用的成果。传统隐私权保护中,个人通过自身隐藏或披露其隐私满足需求;

---

[34] 参见中共中央办公厅、国务院办公厅《国家信息化领导小组关于电子政务的指导意见》,另外三库为法人单位基础数据库、空间地理与自然资源基础数据库、宏观经济基础数据库,载 http://www.e-gov.org.cn/ziliaoku/news004/201305/140983.html,最后访问时间:2015年4月30日。

[35] 《〈2014年联合国电子政务调查报告〉在京发布》,http://politics.people.com.cn/n/2014/0812/c1027-25452028.html,最后访问时间:2015年4月30日。

[36] 郭道晖《论立法中的利益分配与调节》,载《湘江法律评论》(第二卷),湖南出版社1997年版,第10页。

而个人对信息利用需求的满足则需要整个社会信息资源、信息产品和服务的供给，这已经渗透在信息社会个人日常生产和生活之中。这就表明，个人既存在着对其个人信息保护的需求，也存在着利用信息包括利用他人个人信息的需求。

(2) 信息业者对个人信息的利用需求

伴随着社会信息化的进程，信息业者大量出现：不仅传统产业经营者通过大量收集和处理个人信息提高营销回应率、把握市场需求，而且出现了专门以信息的收集、处理、储存、利用和传输为主要业务的信息服务提供者。在传统隐私权保护中，对于他人隐私的披露或利用是否正当，是通过知情权、言论自由等与隐私权之间的冲突在具体个案中进行利益衡量，对他人隐私资料的“利用”并未得到社会的普遍认可；而在信息社会，信息业者对个人信息收集和利用的正当性已经得到了立法和社会的普遍承认，促进个人信息的合理利用与保护个人信息是同等重要的立法追求。信息，包括个人信息的可利用性，带来了人类社会前所未有的商业机会。把握这一商业机会，创造更多财富，是信息业者的基本利益需求。

信息业者并不能一味追求个人信息最大限度的利用，适当水平的个人信息保护也符合信息业者的利益。只有在个人信息能够获得适当保护时，才有可能培植消费者的信任，作为消费者的个人才能放心提供其个人信息，整个商业领域内个人信息的利用才得以进行。同时，个人信息法律保护也是为信息业者收集、存储、处理、利用和传输个人信息活动设定正当性守则，维护信息业者之间的正当公平竞争，避免不当竞争造成劣币驱逐良币的不良效应。

(3) 政府对个人信息的利用需求

政府一直是最大的个人信息收集、处理、储存和利用者，可以说，政府公权力所及之处必然涉及上述个人信息的收集、处理和利用。不同于传统隐私权保护中政府超然的中立地位，在个人信息保护和利用中，政府积极加入其中，具有了利用者和管理者的双重身份角色：一方面，政府作为社会管理和社会福利的承担者，公共安全、公共管理和公共福利的推进都离不开对居民个人信息的掌握；另一方面，出于对行政效率的追求，也会不断促使政府积极探索个人信息利用的限度和价值。

与此同时，政府作为国家政权的承担者，负有保护公民基本权利和自由的责任。“人权是我们时代的观念，是已经得到普遍接受的唯一的政治与道德观念。”[57]政府不能无节制地肆意收集和利用个人信息，个人信息法律保护制度的发展始终伴随着对政府权力的限制。这是因为个人信息法律保护制度的构建不仅是对公民提供保护，而且是为维护政府自身政权合法性所必须。宪法中确立的人权保障原则，需要部门法予以实现：国家通过立法对政府自身和信息业者的个人信息收集、处理和利用能力进行限制，确保本国的人权保护水准，维持自身政权的合法性；同时来取一切必要手段，包括法治、技术和物理措施保障个人信息的安全。

---

[57] [美] L. 亨金《权利的时代》，信春鹰、吴玉章、李林译，知识出版社 1997 年版，前言第 1 页。

3. 个人信息保护与利用的利益衡量

通过以上个人信息保护与利用的利益识别分析不难发现,相较于传统隐私权保护,个人信息保护与利用所涉利益主体和利益内容更加多元化:首先,信息业者和政府作为信息利用角色的加入,将个人信息保护与利用的利益衡量放置于整体社会环境中进行,个人信息保护与利用的社会性使得其不同于传统隐私权保护中个体层面的利益衡量。在社会信息化进程中,传统产业信息化和专门信息服务业出现,使得信息业者作为新的独立利益主体出现;国家除了传统隐私权保护时期中立超然的裁判者身份外,为完成公共管理和公共服务职能,政府大量参与个人信息的收集、处理和利用过程,国家同时具有了管理者和利用者的双重身份。新的利益主体和角色的出现代表了整个社会对于个人信息的利用诉求,因而不同于传统隐私权从个体出发为个体提供单一向度的权利保护,个人信息需要从保护和利用两个角度兼得的视角加以考量。其次,在个人信息利用语境下考量个人信息的保护问题时,传统隐私权保护中的利益冲突仍然存在,个人的隐私利益仍然是个人信息保护利益衡量的重要内容。同时,在信息化背景下,信息业者和政府作为新的利益主体可能在利用个人信息时造成对信息主体的隐私权侵犯,个体的隐私保护需求构成了信息业者和政府利用个人信息的内在限度。"迅猛发展的信息产业和日趋复杂的信息技术加快了人们平衡威斯汀教授四个要素的步伐,推动着隐私法的发展。"[38]在新的社会利益格局之下,需要对个人信息的保护和利用问题进行新的利益衡量。

三、"两头强化,三方平衡"理论的提出

(一) "大数据"之下个人信息保护与利用多赢的新思维

面对利益的多元化及其冲突化,需要借助立法的利益衡量实现对利益关系的调节,使得各个利益主体能够各得其所、各安其位。立法者的利益衡量需要遵循一定的价值导向指引。除了法律普遍适用的公平正义观之外,社会发展所处历史阶段的制约因素实际上构成了影响立法者利益衡量的首要指标。

近20年来,商务智能、社交网站、无线传感器、云计算、语义网等新技术的应用渐次普及,数据呈现爆炸式的增长和累积,大数据[39]成为现实。美国技术活动家尼古拉斯·尼葛洛庞帝教授在《数字化生存》将这一阶段称为"后信息时代"。信息技术推动网络发展,将人们的生活空间从物理空间拓展到电子空间、数字空间,并将逐步造就一个虚拟世界。[40] 互联网改变了人们的表达方式和识别方式。在网络世界里,个人的任何行为都会留下"数据痕迹"。将

---

[38] [美] Martin E. Abrams:《新兴数字经济时代的隐私、安全与经济增长》,温珍奎译,载周汉华主编《个人信息保护前沿问题研究》,法律出版社2006版,第5页;美国信息隐私权学者Alan F. Westin教授在其著作《隐私与自由中》提出社会中相互制约的四个隐私要素,即独处、袒露、好奇、维持公共秩序的政府监控。

[39] 对于大数据尚未有一个公认的定义,比较有代表性的是3V定义,即认为大数据需要满足3个特点:规模性(Volume)、多样性(Variety)、高速性(Velocity)。参见孟小峰、慈祥《大数据管理:概念、技术与挑战》,载《计算机研究与发展》2013年第1期。

[40] 参见张康之、向玉琼《网络空间中的政策问题建构》,载《中国社会科学》2015年第2期。

数据挖掘、整合和分析技术应用于“数据痕迹”，聚合的数据痕迹带来的“隐形”数据和隐私暴露问题，使得后信息时代个人隐私保护面临更多的威胁，个人信息保护更为急迫。另一方面，在后信息时代，时刻都有大量数据产生、流动，数据已经是直接的财富和社会资源，借助数据技术的应用，可以发现新的知识、创造新的价值，实现从数据到知识、从知识到行动的跨越，公私领域对于数据利用的需求也比以往任何一个时代更为迫切。

数据隐私问题也成为数字经济时代的顶层问题，[41]问题解决的关键仍然在于个人信息保护与利用的利益衡量：信息业者和政府作为新的利益主体代表了利用个人信息的利益诉求，构成利益衡量的一个维度；而传统隐私权保护问题仍然存在并更加紧迫，切实保护个人隐私构成了利益衡量的另外维度。在个人隐私保护和个人信息利用都亟待强化的需求格局下，可行的方案是以一定标准实现对个人信息的区别保护和利用，从而实现保护和利用的多赢。

（二）“两头强化，三方平衡”理论的内涵

1. 两头强化

“两头强化”是指建立“个人敏感隐私信息”的概念，在个人敏感隐私信息与个人一般信息区分的基础之上，通过强化个人敏感隐私信息的保护和强化个人一般信息的利用，调和个人信息保护与利用的需求冲突，实现利益平衡。

区分不同的个人信息以划定保护和利用程度的不同，在个人信息法律保护中并不陌生。1981 年欧洲理事会《有关个人数据自动化处理之个人保护公约》第 6 条[42]首次确立了特殊类型的数据保护制度，原则上禁止该类数据的收集和利用，该制度也为之后的欧盟《个人数据保护指令》所沿用。[43] 另外，在欧盟成员国之外，瑞士、挪威、冰岛、加拿大以及我国澳门、台湾地区的法律也存在禁止或限制处理特定类型信息的规定。2003 年，由周汉华教授起草的我国《个人信息保护法（专家建议稿）》对敏感个人信息问题进行了深入研究，但最终未采纳敏感信息概念，“原因在于域外立法中提及的敏感的个人信息所包含的范围非常广泛，但其中很多不适合我国国情。”[44]

“资料敏感性的高低不同，资料处理对个人资料隐私造成风险的大小也各异。”[45]特殊类型数据的概念旨在服务于其规则适用，特殊类型数据与一般数据区别的目的在于适用不同的保护和利用规则，预警某些特殊类型的个人信息需要法律的特别保护，同时给其他个人一般信息的利用松绑，更好地调和个人信息保护与利用的利益冲突。不同类型的个人信息对于实现主体的利益需求的影响不同，以此为导向对个人信息加以类

---

[41] 参见何治乐、黄道丽《欧盟〈一般数据保护条例〉的出台背景及影响》，载《信息安全与通信保密》2014 年第 10 期。

[42] 《有关个人数据自动化处理之个人保护公约》第 6 条规定：泄露种族血缘、政治见解、宗教或者其他信仰的个人数据，关于健康或性生活的个人数据，原则上不得进行自动化处理，除非国内法规定了适当的保护措施。此规定同样适用于犯罪记录。

[43] *See* Directive 95/46/EC, Article 8; General Data Protection Regulation, Article 9.

[44] 前引④，周汉华书，第 79 页。

[45] 孔令杰《个人资料隐私的法律保护》，武汉大学出版社 2009 年版，第 213 页。

型化,实现个人信息保护与利用中多方主体的利益平衡。笔者认为,我国未来个人信息保护法应当以“个人敏感隐私信息”概念对个人信息进行类型化区分。

(1)强化个人敏感隐私信息的保护

所谓个人敏感隐私信息是指关涉个人隐私核心领域、具有高度私密性、对其公开或利用将会对个人造成重大影响的个人信息,如有关性生活、基因信息、遗传信息、医疗记录、财务信息等个人信息。我国《个人信息保护指南》中将“敏感信息”界定为“一旦遭到泄露或修改,会对标识的个人信息主体造成不良影响的个人信息。”[46]笔者认为,以“会对个人信息主体造成不良影响”作为界定标准,失之过宽,也使得敏感信息与一般信息的区分意义大打折扣。在个人信息保护法中,法律并非为所有涉及隐私的信息都提供高强度的保护,而应仅限于个人敏感隐私信息。个人信息与个人隐私之间存在交叉关系,有关私生活秘密构成二者的交集。数字化技术的应用使得越来越多的个人私生活秘密可以被记录而具备个人信息的特点,数据挖掘、分析和整合技术的应用使得几乎所有个人信息都与隐私相关,如果以个人隐私为标准进行区分保护,将对个人信息的利用产生实质限制的效果,也会导致对言论自由和社会公开的不当压制。信息社会中,任何人都已经离不开信息产品和服务,允许非敏感隐私信息的利用,最终也使得每一个信息主体受益。

敏感隐私信息的概念是极具本土化色彩的概念,在我国进行敏感隐私信息的类型化列举时,应注意主要以我国文化传统、社会普遍价值观、法律传统、风俗习惯等作为考量因素。我国台湾地区的《个人资料保护法》提供了极具价值的参考:该法第6条以是否与个人核心隐私相关作为标准,对个人敏感信息进行了类型化列举,包括“有关医疗、基因、性生活、健康检查及犯罪前科之个人资料”。同时,个人敏感隐私信息是一个动态范围,还应结合当下科技发展水平、社会发展动态等灵活修正其列举类型。2012年欧盟《个人数据保护条例》中就适应现代生物科技的发展水平,将基因信息列入特殊类型的数据之中,给予特别保护。[47]

(2)强化个人一般信息的利用

2011年5月,全球知名咨询公司麦肯锡(Mckinsey and Company)发布了《大数据:创新、竞争和生产力的下一个前沿领域》报告,这是全球范围内从经济和商业维度诠释大数据发展潜能的第一份专题研究成果。该报告指出“数据已经渗透到每一个行业和业务职能领域,逐渐成为重要的生产因素:而人们对于海量数据的运用将预示着新一波生产率增长和消费者盈余浪潮的到来。”[48]大数据及其技术的应用,将使人类的决策空前智能化、精

---

[46] 国家质量监督检验检疫总局、国家标准化管理委员会《信息安全技术 公共及商用服务信息系统个人信息保护指南》第3.7条。

[47] *See* General Data Protection Regulation, Article 9.

[48] MCKINSEY GLOBAL INSTITUTE, BIG DATA: THE NEST FRONTIER FOR INNOVATION, COMPETITION AND PROBUCTIVITY, at http://www.mckinsey.com/, (Last visited on April 30, 2015).

确化。[49] 大数据之“大”,不仅在于规模,更在于价值,越来越多的人将数据视为一种经济资产看待。政府可以通过精确的数据量化更好地了解国民经济和社会的运行状况,更好地决策;经营者可以从数据中了解消费者的爱好、特点、心理特征,从而提供更具个性化的产品和服务,实现经营者和消费者的双赢;另外,个人在真实物理世界的活动得到了前所未有的记录,新闻跟帖、社交平台互动记录、网络浏览记录等等都为社会科学的研究提供了大量的数据,21 世纪的社会科学可能实现定量化的研究,脱下“准科学”的外衣,成为一门真正的科学。因此,强化个人一般信息的利用,最大程度地促进其商业和公共管理价值的发挥,已经成为各国占据后信息时代话语权的必然选择。我国将要制定的个人信息保护法,必须给予信息业者收集、处理和利用个人信息的较大自由;必须保证国家机关为了国家安全和社会管理之目的,收集、处理和利用个人信息的权力和能力。

2. 三方平衡

“三方平衡”是指个人对个人信息保护的利益(核心是人格自由和人格尊严利益)、信息业者对个人信息利用的利益(核心是通过经营活动获取经济利益)和国家管理社会的公共利益之间的平衡。平衡是一种张力状态,各利益主体的核心利益得到保护和实现,并让渡非核心利益作为他方实现其核心利益的条件和基础。具体而言,个人信息中涉及敏感隐私的部分,其保护应该得到强化,个人的人格自由和人格尊严应该得到更高水平的保护;而就个人一般信息,信息主体做出一定让渡,让信息业者得到收集、处理和利用的更大自由,以利其经营。就信息业者而言,其通过个人让与的利益以及国家保障的良好信息化经营环境,实现其经营的主要利益;同时,信息业者尊重个人的隐私权和国家的管理规定,在收集、处理、存储、传输和利用个人信息的过程中自觉为信息主体的核心隐私提供保护,并且以尊重隐私为导向,自觉抵制以侵害隐私为目的信息技术的研发和应用,实现信息主体的核心利益和国家在个人信息保护秩序中的公共管理利益。另外,正是信息业者提供的各种信息产品和服务,使得个人更有机会满足日常生活需要和实现知情权。就国家而言,一方面为了满足社会管理之目的,应当获得收集、处理、储存和利用必要的个人信息的权力和能力,另一方面公权力的行使也需要约束,不过分利用技术手段和国家机器干预私人生活,对其个人信息的收集利用等方面的权力和能力加以规制和约束;同时,国家作为公权执掌者,还需要通过制定法律为隐私权保护划定边界,为信息业者的经营活动制定包括公平竞争在内的管理规范,为个人信息数据库的建设及其安全包括物理安全与信息安全提供一切必要的条件和制度保障,打击严重侵害个人信息的犯罪行为,处罚信息业者不当收集、处理、存储、利用和传输个人信息的行为。

---

[49] 例如,2008 年谷歌推出”流感趋势”的服务,该服务器通过数学模型对谷歌服务器中保留的数据进行测算,实现流感预测,其速度甚至比美国疾病控制和预防中心还要快 7-10 天,参见《谷歌推出“流感趋势”服务,可预测流感疫情》,载 http://tech.qq.com/a/20081112/000333.htm,最后访问日期:2015 年 4 月 30 日;百度 2014 年推出“百度迁徙”服务,通过对百度地图的请求数据挖掘分析,以可视化方式全程、动态展示了我国春节前后人口大迁徙的轨迹与特征,2015 年新版“百度迁徙”还新增实时航班、机场热度和火车站热度等查询功能,方便网民、企业的生活和生产,参见《“百度迁徙”春运上线,携手央视创新大数据新闻》,载 http://it.sohu.com/20150215/n409037209.shtml,最后访问时间:2015 年 4 月 30 日。

四、“两头强化,三方平衡”理论的实现

(一) 作为我国个人信息保护立法的理论基础

就个人信息的立法模式而言,存在着欧盟和美国两大立法模式。美国采取经营者自律模式与其原有的隐私法律保护比较完备有关,欧洲采用国家(政府)主导的立法模式则与其立法传统有关。而我国目前隐私权保护的一般制度尚未全面建立,有关个人信息保护的法律规定零散混乱,有必要制定一部全面的个人信息保护的法律,对个人信息保护与利用的基本问题加以规范。

“法律的主要作用之一就是调整及调和种种相互冲突的利益,无论是个人的利益还是社会的利益。”[50]在现代国家体制下,利益衡量应当主要是立法的工作,解决规范背后的利益冲突的体系构成法的内在体系,[51]能够担纲个人信息保护法立法理论基础也必然是旨在调和个人信息保护与利用中多元利益冲突的利益衡量问题。

在信息社会中,围绕“个人信息”资源,存在个人、信息业者和国家三方利益主体,通过“个人敏感隐私信息”的概念实现对个人信息的类型区分,强化“个人敏感隐私信息”保护,以维护个人在个人信息保护中的核心利益;通过强化“个人一般信息”利用,以满足信息业者和国家利用个人信息的正当需求,实现“三方平衡”。未来我国个人信息保护法应当将“两头强化、三方平衡”理论作为其理论基础,并以此为指导构建个人信息保护与利用的相关制度。

(二) 确立国家主导、行业自律与个人参与的法治模式

1. 国家主导

个人信息保护法中的国家主导体现在立法和执法两个方面:首先,制定统一的个人信息保护法,作为个人信息保护的基本法律调整公私领域内的个人信息保护与利用关系。“制定法权威性、强制性与普遍适用性等优势是自律规范等非正式制度无法企及的,它能够为机构和个人建立稳定的预期从而更加有效地规制其行为。”[52]尤其是在我国尚未形成充分的市场自律氛围的情况下,由国家统一立法加以规范尤为必要。具体说来,以“两头强化、三方平衡”理论为立法指引,通过规定适合我国国情的个人信息保护的基本原则、信息主体的权利、信息业者和政府的义务、法律责任等,确立我国个人信息保护的门槛标准。其次,国家主导还意味着通过专门机构负责个人信息保护法律的执行、监督等各方面事务。专门数据保护机构的设置源于欧盟,[53]在其影响下,瑞士、挪威、加拿大、我国香港和澳

---

[50] [美] E·博登海默《法理学:法律哲学与法律方法》,邓正来译,中国政法大学出版社 1999 年版,第 398 页。

[51] 参见 Philipp Heck, Begriffsbild ung und Interessenjurisprudenz, Tübingen., S. 139ff.;转引自朱岩《社会基础变迁与民法双重体系建构》,载《中国社会科学》2010 年第 6 期。

[52] JAMES G. MATCH & JOHAN P. OLSEN, REDISCOVERING INSTITUTIONS: THE ORGANIZATIONAL BASIS OF POLITICS, New York: The Free Press, 1989, p. 178.

[53] *See* Directive 95/46/EC, Article 28.

门特区等也设立了专门的数据保护机构。笔者认为,我国应当建立独立的专门管理机构,确保我国个人信息保护法的实施。同时,在全球经济一体化背景下,该专门管理机构也有利于我国在个人信息跨国流通过程中更好地参与国际合作,维护我国国家信息主权和公民的信息利益。就我国目前的机构设置现状来看,可以考虑以现有的国家互联网信息办公室为平台,适当整合信息产业、工商管理等部门的部分职能,建构该专门管理机构,由其负责监督个人信息保护法的实施、展开个人信息保护执法调查、进行个人信息保护与利用研究等,并适时向立法机关提出立法意见和建议等。

2. 行业自律

在国家主导之下,还应该充分鼓励信息业者的行业实行自律管理。自律机制是指在国家立法之外,社会组织体自发通过确立自律规范来规范自己行为实现自律目的的一种机制。[54] 作为一种内在机制,自律机制可以与国家法律的外在强制机制实现良性互动。统一的个人信息保护法往往缺乏灵活性和针对性; 多方利益平衡和妥协之后的立法,可能仅能在个人信息保护的最低标准上达成共识。因此,在个人信息保护方面行业自律有更大的发挥余地,应当充分调动和鼓励同行业者自律的积极性,鼓励业者承担"超越法律"的社会责任。[55] 具体而言,一方面信息业者可以参照国家个人信息保护基本法的原则性规定,结合自身的业务特点和业务实践经验,制定更具针对性更为细致的个人信息保护与利用准则,以简明和易于信息主体理解的方式在开展具体个人信息处理业务时,向信息主体加以提示和说明,为信息主体提供更为便利、充分、高水平的保护。另一方面,行业自律还是有效缓解信息技术快速发展所引起的立法供给不足问题的途径。整个社会仍然处于信息化进程之中,这要求立法必须理性而有节制,不能成为整个市场技术创新的阻碍。鼓励信息行业制定自律性规范,为信息主体提供一定保护,立法者在充分总结信息业者有益经验的基础上再适时制定法律加以规范,不失为避免盲目和超前立法扼杀技术创新活力的良策。同时,来自市场的动力和压力为行业自律提供了足够动力: 信息保护水平将影响消费者选择,消费者"用脚投票",实现业者的优胜劣汰; 声誉机制也为信息行业的自律提供了反向激励。

3. 公民参与

随着我国社会管理方式的创新,政府由管制型政府向服务型政府转型,对于社会问题的治理,我国也不再单纯强调国家管制,而是致力于国家管理、社会协同和公民参与的合作管理。在个人信息保护问题上,公民存在广泛的参与热情和需求,现代信息技术发展也为扩大公民参与提供了便利条件。"不透明、缺乏参与会使规则本身的合理性存在疑问,难以跟上社会进步的步伐,最终必然会导致特别规则与政府干预越多,秩序与自治越少的二律背反现象。"[56]因此,在相关法律政策制定、执行和救济的各个环节都可

---

[54] 参见齐爱民《个人信息保护法研究》,载《河北法学》2008 年第 4 期。

[55] 指企业负担的那些超出法律强制性义务规定且符合社会价值和期望的责任。参见周林彬、何其丹《试论"超越法律"的企业社会责任》,载《现代法学》2008 年第 3 期。

[56] 周汉华《论互联网法》,载《中国法学》2015 年第 3 期。

以借助网络平台等方式拓宽公民参与途径,强化公民利益表达、救济和监督:首先,在法律和政策制定过程中,除传统的立法听证之外,立法机关和行政管理部门还可以通过开放网络平台征求社会公众意见。现代社会利益日渐多元化,民选代表难以充分表达公众的利益诉求,通过网络平台征求意见可以将更多的利益诉求表达纳入立法者考量范围,以制定更加正义的法律政策。其次,个人信息保护专门机构也可以建立网络平台,为信息主体提供更为便捷的举报、投诉、申诉、监督方式,确保法律和政策得到切实实施,为进一步完善相关法律和政策进行长期准备。最后,政府部门和信息业者也应当通过建立相应网络平台、市民热线等方式,听取公众意见并及时反馈,及时发现问题以实现更好的治理。

(三)信息业者实名制和网络用户真实身份可查验制

为净化网络环境和维护网络安全,我国逐步从电信增值服务提供商、网络服务提供者实名制[57]推广为全网用户实名制,以加强网络环境管理。[58] 对电信增值服务提供商、网络服务提供者等信息业者的实名制为管理应有之义,其必要性与正义性是显然的;而全网用户的实名制引起了较大争论。笔者认为,切实落实信息业者的实名制和合理构建用户真实身份可查验制,最终将助力于公民个人信息的保护和利用。

1. 信息业者实名制

电信和互联网极大地便利了信息发布,但随之而来的钓鱼网站、伪基站所发送的垃圾短信和邮件以及欺诈电话通信,严重扰乱了社会秩序和民众的日常生活,其中最为严峻的是虚拟号码拨号(伪基站)和钓鱼网站[59]等电信诈骗和网络诈骗行为,造成公民财产乃至人身损害,损及国家公权力机关威信和整个市场环境的信任秩序。无论虚拟号码拨号还是钓鱼网站,都与电信运营商、中国互联网络中心(CNNIC)对于信息业者真实身份的动态监管不力有关。虚拟号码拨号之所以能够成功,是利用了电信运营商 IP 电话业务漏洞,实现将主叫号码设置为具有公信力的国家机关和社会机构的号码;而对于钓鱼网站,目前主要是由中国反钓鱼联盟、反诈骗联盟等组织通过其联盟单位开放数据库进行疑似恶意网址比对,以降低联盟单位的用户遭受网络诈骗的几率,而中国互联网络中心在建立综合联动的动态反钓鱼机制、网站身份诚信认证等方面作为有限。切

---

[57] 2000 年国务院《互联网信息服务管理办法》,规定经营性互联网信息服务提供者实行许可制;2005 年信息产业部《非经营性互联网信息服务备案管理办法》,规定非经营性互联网信息服务网站实行备案制;2002 年信息产业部出台《中国互联网域名管理办法》,规范在我国境内从事的域名注册服务及相关活动;2005 年信息产业部发布《互联网 IP 地址备案管理办法》、《互联网站管理细则》,对互联网 IP 地址及网站备案进行了规定。

[58] 2010 年 9 月以来,工信部推进电话及移动电话用户实名登记制度,2013 年《电话用户真实身份信息登记规定》将电信用户实名制度化;2015 年国家网信办发布《互联网用户账号名称管理规定》,其中第 5 条明确我国就网络用户采取"后台实名、前台自愿"制度。

[59] 虚拟号码拨号多体现为犯罪分子将主叫号码设置为金融、电信甚至国家行政、司法机关等具有公信力的主体,以此取得被害人信任而实施诈骗行为;钓鱼网站是犯罪分子仿冒的网页,通常是知名购物网站,然后通过邮件、短信、网页广告等形式大量发送含有该网站地址的内容发送给受害人,因其网址、网页内容等与被仿冒网站存在极高相似度,被害人可能基于误信而提供如银行账号密码等个人信息而遭受损失。

实落实信息业者的实名制，不仅要求相关监管部门在入网环节拦截不适格主体，更重要的是切实进行动态监管，维护网络秩序的可信度。

2. 用户真实身份可查验制

用户真实身份可查验制与网络用户实名制相关，可以视为是实名制的升级版，二者都旨在建立网络虚拟身份和物理真实身份之间的联系，改变网络身份的虚拟性和易变性导致的网络违法犯罪行为难追踪追责现象。网络世界并非法外空间，同样需要国家管理维护网络秩序安宁，这是实名制的正当性所在。用户真实身份可查验制与用户实名制具有同样的网络管理效果，但其优点在于其可以更好地维护公民个人信息安全，避免实名制引发“寒蝉效应”，最大限度地减少对公民权利和自由的限制，实现管制与自由的平衡。具体说来，用户真实身份可查验制度是通过建立国家官方网站进行公民真实身份验证，统一发放“网络身份识别码”，以认证“网络身份识别码”代替实名制之下的公民真实身份识别。[60] 在用户真实身份可查验制之下，网络用户真实身份仅由唯一国家网站掌控，相较于实名制之下提供给形形色色的互联网信息服务提供者而言，大大缩减了“公开”范围；同时，相较于互联网信息服务者的参差不齐，国家网站的安全维护水平可以做到更高一些。另外，用户真实身份可查验制度之下，用户“实名”仅存在于该国家网站之中，并且限于符合法律规定的正当事由和程序才可进行用户真实身份的查验，最大限度维持了用户在网络空间里的“匿名”状态，避免“寒蝉效应”对公民言论自由产生不利影响。国家机关也只有在有法律依据、符合授权的情况下，对于涉及违法、犯罪行为的网络用户进行实名查验，不得滥用权力查验网络用户的真实身份，而对于一般性质的不当网络言论和行为不应动辄动用国家公权力查验网络用户的真实身份。

（四）强化国家对个人信息的保护与利用的双重职能

在大数据背景下，最大化实现国家对个人信息利用的方式便是建立国家中心数据库，解除数据库之间的“信息孤岛”状态，最大限度地提升政府行政管理效率。2015 年 4 月 13 日，中共中央办公厅、国务院办公厅对外公布《关于加强社会治安防控体系建设的意见》（以下简称《意见》），《意见》第 10 条指出，我国将建立以公民身份号码为唯一代码、统一共享的国家人口基础信息库，建立健全相关方面的实名登记制度，建立公民统一社会信用代码制度，并探索包含公民所有信息的一卡通制度。

国家中心数据库是社会信息化发展和进步的必然，而如何实现《意见》中指出的“确保信息安全、保护公民合法权益前提”则是我们需要面对的首要问题。笔者认为，该问题的解决包括个人信息的安全和国家权力的限制两个方面，应当通过技术保障和法律规制相结合确保个人信息资源的安全共享和正当利用。国家必须加大技术投入，致

[60] 具体说来，网络用户首先在国家官方网站上提供自己的真实身份信息或者使用二代身份读取身份证信息进行注册，由该官方机构对网络用户的个人信息进行识别、验证，通过验证后，网络用户将获得一个唯一、随机序列识别码及相应密码，以该识别码作为该网络用户的网络身份识别码代替个人真实身份信息申请其他注册服务。随后，在网络用户在其他网站进行注册时，仅需要向网络服务提供者提供该识别码，网络服务提供者通过访问国家官方网站对用户的识别码和密码进行验证，验证通过后向其提供服务。

力技术创新,提升我国信息安全水平,确保我国信息主权安全,从技术层面上确保国家中心数据库和所有国家机关涉及公民个人信息数据库的安全;更重要的是通过法律严格限制政府公权力,确保国家机关对国家中心数据库的正当利用,避免"数据监控"的噩梦。国家中心数据库的建立本质上是扩张公权力对公民私生活的介入,必须符合法律保留原则、符合目的性原则和比例原则。首先,国家中心数据库的建立涉及到公民基本权利和自由,必须由立法机关立法,制定明确的法律依据。在立法时,关键在于严格限制该数据库的利用,只有重大社会公共利益方能构成利用的正当性理由,在立法中明确利用该数据库的具体情形和前提条件。其次,国家中心数据库中个人信息收集和利用,必须满足符合目的性原则要求,不得在法律规定的目的之外收集和利用个人信息。再次,国家中心数据库的利用对于其欲达目的而言必须是必要和重要的,符合比例性原则,也即"对于当事人自由的干预应尽可能最少"[61]。对于尚未构成违法犯罪行为、并非严重背离社会公序良俗的行为,国家应当抱有包容的心态,给予民众充分的自由,追求良治、善治,而非一味监控管制。最后,国家中心数据库中的个人信息的收集和利用,还需要遵循个人信息保护与利用的基本原则,包括数据质量、限制收集、公开原则、信息主体参与等,确保公民的知情权和参与权,将国家中心数据库的运作情况作为政务公开的重要内容加以公开,便于公众和社会进行监督。

(五)信息业者:去个人化的信息处理与利用

个人信息是"可以识别个人身份的信息",识别性因素会对信息主体的权益保护和业者的利用产生影响。一方面,对于直销等针对特定信息主体利用个人信息时,对于信息业者的个人信息利用行为,应当施加更多的限制[62];另一方面,当信息业者并非追求针对特定信息主体"一对一"利用个人信息时,应当在其收集、存储、处理和利用个人信息的过程中进行去个人化处理。例如,个人信息用于定向营销、数据库营销和商务智能分析中,信息业者关注消费者的群体特征,去除单个个人的明确身份识别要素并不影响信息业者对消费者群体特征的分析。除得到信息主体同意的情况外,信息业者一般应当通过代号化或加密处理,去除个人信息的可识别性因素,切断信息与特定个人之间的辨识要素,实现信息的去个人化,降低未来可能的信息泄露等安全事件对信息主体的影响。

去个人化会引起经营者的信息处理成本小幅增加,但去个人化之后个人信息处理、传输和利用不当的风险将显著降低,能够避免信息主体可能遭受的直接识别的侵害,对信息主体具有积极意义,也是最大限度地在业者和信息主体之间实现个人信息的保护和利用需求。

(六)个人:未成年人和敏感隐私信息的特殊保护

1. 强化对未成年人信息的保护

根据中国互联网络信息中心发布的《2013 年中国青少年上网行为调查报告》显示,截至 2013 年 12 月,中国未成年网民规模达 1.4 亿,在整体网民中的占比为 22.65%,互

---

[61] 参见陈新民《德国公法学基础理论》(下册),山东人民出版社 2001 年版,第 358 页。

[62] *See* Directive 2002/58/EC, Article 13.

联网在 12 岁以下的少年中的渗透加大，其上网行为涉及信息获取、交流沟通、网络娱乐、商务交易等方面。[63] 2014 年是我国接入国际互联网 20 周年，如今的未成年人是真正成长于网络环境中的一代，网络是其生活的重要内容，互联网深刻影响着他们的生活方式甚至思想意识。与成年人相比，未成年人心智尚未成熟，没有足够的认识能力和控制能力，也缺乏足够的自我保护能力，其权益无疑更容易受到侵害，在个人信息保护与利用方面，更应为未成年人提供特殊保护。

在强化未成年人个人信息保护方面，美国是立法先驱。早在 1998 年美国就制定了《儿童网络隐私权保护法》，限制网站运营商通过互联网收集儿童个人信息。该法规定网站营运商负有保护儿童网络隐私和安全的责任，不经儿童父母或监护人的同意，不得收集 13 岁以下儿童的个人信息；到 2012 年，网站运营商限制收集的范围扩张到 13 岁以下儿童的照片、视频和地理位置信息。此外，美国一些州的立法也体现了强化未成年人保护的理念，如 2013 年美国加州《橡皮擦法案》要求社交网站应允许未成年人擦除自己的上网痕迹，以免其未来面临其在心智尚未成熟时留有的网络痕迹的困扰。[64] 欧盟 2012 年《个人数据保护条例》也借鉴美国的立法经验，增加了儿童个人数据的特殊保护规定。[65]

我国《个人信息保护指南》也体现了对未成年人个人信息予以特殊保护的理念，规定“不直接向未满 16 周岁的未成年人等限制民事行为能力或无行为能力人收集个人敏感信息，确需收集其个人敏感信息的，要征得其法定监护人的明示同意”。应当说，《个人信息保护指南》不局限于网络环境而统一为未成年人个人信息收集提供强化保护，是相较于美国和欧盟立法的进步之处，因为随着新型数字媒体平台、电视购物等的发展，对未成年人个人信息的收集和利用肯定不会仅仅发生在网络环境中；但同时《指南》将这种针对未成年人群体的强化保护又局限于未成年人敏感信息的收集，实际上是限缩了对未成年人强化保护的效力。同时，在未来我国个人信息保护立法进程中，还应当通过大量的社会实证调研，确定一个适合我国青少年发展状况的强化保护的年龄节点。

2. 强化个人敏感隐私信息的保护

敏感隐私信息概念的提出在于为个人敏感信息提供强化保护，对敏感隐私信息和一般信息的收集、处理和利用适用不同的法律规则。从比较法上的经验来看，欧盟在明确区分二者的基础上原则性禁止个人敏感信息的收集和处理。美国虽然不存在明确的敏感信息分类，但是也存在一些类似的限制性规定，体现在不得以敏感信息作为做出某些决定的依据，否则将被视为歧视性决定。如在美国征信行业中，征信机关虽然可以收集种族、国籍、婚姻状况等敏感信息，但是不得进行传播，也不得在进行信用计分时加以考虑或计算，否则会被联邦贸易委员会视为歧视性决定而受到惩罚。

个人敏感信息的强化保护也仍然包括保护和利用两个维度，保护体现在原则上禁

---

[63] 参见中国互联网信息中心《2013 年中国青少年上网行为调查报告》，载 http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/，最后访问日期：2015 年 4 月 30 日。2014 年中国青少年上网行为调查报告尚未发布。

[64] 参见裴洪辉《美国推“橡皮擦”法案，抹掉未成年人的网络过失》，载《法律与生活》2014 年第 1 期。

[65] *See* General Data Protection Regulation, Article 8.

止处理,而利用则体现在对禁止处理的例外规定。禁止处理的原则应当适用于个人信息处理的全过程,包括收集、存储、处理、利用及传播等各个环节。禁止处理的例外限于信息主体明确同意或自行公开、法律明文规定、公务机关执行法定职务或非公务机关履行法定义务所必要、公务机关或研究机构基于医疗、卫生、预防犯罪等目的为统计或学术研究必要等情形。同时,在上述例外利用的情形中,进行个人敏感信息处理的公私机构应当为个人敏感隐私信息提供更高水平的安全保障。

结 论

进入信息社会,每一个人都是"信息人",个人既是信息的生产者也是信息的消费者,任何人都不可能离开信息而生存。与此相适应,人类社会中的每一种社会关系都直接或间接打上了"信息化"的烙印,调整这些社会关系的法律也都应成为"信息化"的法律。个人信息与隐私具有千丝万缕的联系,但由于其所具有的人格自由和人格尊严价值、商业价值和公共管理等多重价值,所以对其保护与利用的利益再衡量必然成为个人信息保护法在理论上的起点和基础。

利益博弈中零和游戏的结局是"你死我活",而立法上的利益衡量要达到的目的是"多赢"和"共和"。因此,需要识别个人信息保护和利用中多方主体的利益需求,承认与确保其核心利益的实现,让渡自身非核心利益而使他方的核心利益得以实现。

通过对个人敏感隐私信息强化保护,以及强化个人一般信息的商业利用和国家基于公共管理目的的利用,实现个人、信息业者和国家三方利益平衡。这一"两头强化,三方平衡"理论,应当作为我国个人信息保护法的理论基础。国家主导、行业自律与个人参与的法治模式,信息业者实名制与用户真实身份可查验制,国家作为个人信息利用者与社会管理者双重功能的发挥,信息业者对个人信息的去个人化利用,以及对未成年人个人信息、个人敏感隐私信息的特殊保护等,都是全面实现"两头强化,三方平衡"理论所要求的主要制度安排。

Abstract: The traditional Privacy Protection Act mainly focuses on the interest measurement problems among privacy protection, the protection of expression and the right to know. Although the public interest is the significant constraint, the legislative policies tend to provide absolute protection for individual privacy. The nation not only plays its role as a manager, but also as an independent collector and user of individual information. In the new pattern of interest balancing, our country's Individual Information Protection Law should base on the theory of strengthening two sides and balancing three parts, and design a relevant system project for realizing this theory.

(责任编辑:陈贻健)