

# 个人信息法律保护路径分析

肖少启<sup>1,2</sup>

(1. 韶关学院 法学院, 广东 韶关 512005; 2. 重庆大学 法学院, 重庆 400044)

**摘要:**个人信息权是一项基本的人权。目前,中国对个人信息保护不容乐观,特别在云计算环境下,个人信息被盗用、滥用现象极其严重。个人信息保护问题本身跨越了宪法、行政法、刑法和民法等法律部门的界限,如果仅仅从某个部门法的角度观察它难免会顾此失彼。中国应该制定一部统一的个人信息保护法,确立科学的基本原则,准确界定个人信息法律关系的主体制度,明晰个人信息法律关系的客体制度及其对象,同时构建合理的个人信息权利救济制度。

**关键词:**个人信息;个人信息权;法律保护;立法

**中图分类号:**DF01

**文献标志码:**A

**文章编号:**1008-5831(2013)04-0119-08

自20世纪50年代起,在西方发达国家,学术界及司法实务部门开始关注个人信息保护问题,通过立法建立了旨趣异同的个人信息法律保护模式。中国正大踏步迈进信息社会,个人信息保护问题也越来越引起人们的高度关注和重视。《民法典》的起草和制定工作正如火如荼地展开,个人信息保护的立法也被提上了议事日程。当前,个人信息法律保护面临诸多挑战,例如国际互联网,全球化,无所不在的个人信息及个人信息收集,功能越来越强大的计算机和其他数据处理设备,射频识别、生物识别技术、人脸识别等新技术,日益加强的管制和数据监控(dataveillance),以及越来越频繁的最初并不是为了收集目的的个人数据的使用,尤其是涉及国家安全、打击有组织的犯罪和恐怖主义等<sup>①</sup>。因此,制定一部科学合理的个人信息保护法具有重要的历史价值和现实意义。

## 一、中国个人信息立法保护的现实迫切性

当前,中国对个人信息的法律保护不容乐观。“共享客户资源”在商业界几乎是公开的秘密,一旦个人信息被非法出售,房产代理、各种中介服务公司、广告公司、保险经纪公司、信用卡公司等会时不时电话或短信骚扰客户,个人信息成了这些公司企业的金矿。更有甚者,它们业已形成利用个人信息从事非法获利的黑色链条。

**收稿日期:**2012-12-19

**基金项目:**国家社科基金项目“网络环境下个人信息安全危机与法律对策研究”(12XFX021);中央高校基本科研业务费科研专项人文社会科学类重大项目“政府依法治理网络空间的技术规范和法律规则研究”(CDJKXB12001)

**作者简介:**肖少启(1970-),男,湖南衡阳人,韶关学院法学院讲师,重庆大学法学院博士研究生,主要从事民法学及法学理论研究。

**致谢:**在文章撰写过程中,齐爱民教授给予了悉心指导。在此,笔者表示最诚挚的谢忱!

<sup>①</sup>Korff, Douwe and Brown, Ian, New Challenges to Data Protection - Final Report (January 20, 2010). European Commission DG Justice, Freedom and Security Report. Available at SSRN; <http://ssrn.com/abstract=1636706>.

就个人金融信息保护而言,中国现行法律法规对于银行个人金融信息缺乏有效的保护和明确的规定,有关银行对个人客户信息保护的规定比较零散而且笼统,更多的规定集中于银行对个人金融信息的披露方面,并且授予许多政府部门获取个人金融信息的权力。现行法律中保护银行个人金融信息的内容也过于简陋,仅仅规定了银行负有保密义务,并且这种保密义务也非常笼统,缺乏对个人金融信息权属的确定,个人客户在其信息利益遭受侵犯时无法获得法律上的救济。总而言之,中国对银行个人金融信息保护的相关法律都侧重于公共机构对于个人金融信息的获取而缺乏对有关的权利主体救济方面的规定<sup>[1]</sup>。由此,我们的档案信息几乎得不到有效保护,任何人都可以轻易获取我们的档案材料。身份盗用,即利用个人信息非法获取现有的金融帐户,公开欺诈帐户,或者以他人名义获得信用卡,这些都是增长最快的白领型犯罪活动<sup>②</sup>。

随着传感器网络、生物识别技术、射频识别及监控系统等高科技的发展,个人身份识别、电子病历信息、远距医疗记录、交通讯息、各种消费资金帐户信息载体与日常生活层面应用的异类结合等,都会造成个人信息被大量运用与流通,信息主体本人却被蒙在鼓里,尤其是在虚拟网路的推波助澜下,个人信息被滥用、私权被侵害的程度达到无以复加的程度。新技术的运用使收集和分享个人信息变得更加容易,个人敏感信息(包括生物学鉴定和基因构成等)被频繁收集和使用,公众档案在互联网上遭披露。特别是云计算技术的运用,个人信息的保护问题尤为突出。一般认为,云计算是指一种通过互联网以服务的方式提供动态可伸缩的虚拟化资源的计算模式。根据不同的部署模型,云计算又可分为私有云(private cloud)、公共云(public cloud)、社区云(community cloud)以及混合云(hybrid cloud)等几种。云计算将使未来的互联网变成超级计算的乐土,但同时也是个人信息泄露的温床。由于互联网没有国界的限制,在云计算环境下,数据有可能储存

在世界上任何一个我们根本就无从知晓的数据中心,信息主体把自己的业务放到云端数据中心,安全是个非常严峻的问题<sup>③</sup>。例如,自2005年以来,美国许多机构一并泄露了一亿条以上的记录。一旦信息泄露,人们精神上可能极度焦虑,因为他们无法再进行数据恢复和防止信息资料的下游滥用。而且,一旦信息被不法分子利用,潜在的危害如账户失窃、身份盗用、诈骗、绑架等严重的刑事犯罪将接踵而至<sup>④</sup>。针对这一严峻形势,世界上大约90个国家和地区颁布了法律,赋予个人控制由政府机关和私人机构收集和使用的这些个人信息数据。几个主要国际公约已在欧洲生效,亚非国家正在制定相关法律。国际机构正在制订国际公约,国际法庭也发布了有关的决定<sup>⑤</sup>。

## 二、中国个人信息法律保护的学理分歧

中国目前尚未制定公民个人信息保护的专门法律法规,虽然有近40部法律、30余部法规,以及近200部规章涉及个人信息保护,其中包括规范互联网信息规定,医疗信息规定,个人信用管理办法等,然而内容较为分散,权责不明晰或者存在部门规章效力层级偏低等问题。

对公民个人信息提供何种法律保护或救济,学术界存在几种不同的观点。

其一,刑法保护说。有学者认为,在侵权行为日益猖獗的今天,仅仅以其他诸如民事制裁手段似乎很难遏制这种现象的滋生和蔓延,只有通过刑法这种最严厉的保障手段才能有效地对个人信息权进行保护<sup>[2]</sup>。将公民个人信息纳入刑法保护范畴,将国家机关或者金融、电信、交通、教育、医疗等单位的工作人员界定为本罪主体。同时规定非法获取信息者也可成为本罪主体。因此,中国刑法对本罪在为出售和非法提供信息行为时主要为身份犯,为非法获取信息行为时一般主体可构成本罪<sup>[3]</sup>。笔者认为,对个人信息保护寄予刑法厚望不现实。诚然,中国刑法第253条规定了“出售、非法提供公

②Walker, Robert Kirk, Forcing Forgetfulness: Data Privacy, Free Speech, and the Right to Be Forgotten (March 18, 2012). Available at SSRN: <http://ssrn.com/abstract=2017967> or <http://dx.doi.org/10.2139/ssrn.2017967>.

③Hon, W. Kuan, Hörnle, Julia and Millard, Christopher, Data Protection Jurisdiction and Cloud Computing - When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3 (February 9, 2012). International Review of Law, Computers & Technology, Vol. 26, No. 2-3, 2012; Queen Mary School of Law Legal Studies Research Paper No. 84/2011. Available at SSRN: <http://ssrn.com/abstract=1924240> or <http://dx.doi.org/10.2139/ssrn.1924240>.

④Swire, Peter P., From Real - Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud (April 12, 2012). Ohio State Public Law Working Paper No. 175. Available at SSRN: <http://ssrn.com/abstract=2038871> or <http://dx.doi.org/10.2139/ssrn.2038871>.

⑤Banisar, David, The Right to Information and Privacy: Balancing Rights and Managing Conflicts (March 10, 2011). World Bank Institute Governance Working Paper. Available at SSRN: <http://ssrn.com/abstract=1786473> or <http://dx.doi.org/10.2139/ssrn.1786473>.

民个人信息罪”及“非法获取公民个人信息罪”，但刑法第 253 条所规定的犯罪主体局限于特殊主体，即国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，而对于其他一些主体如互联网公司、汽车厂商、房地产中介机构、宾馆酒店等单位和机构则排除在外。目前，利用刑法作为主要的法律手段打击个人信息滥用的犯罪行为效果不佳。一方面，执法官员缺乏足够的资源来指控身份盗用行为；另一方面，与暴力犯罪和毒品犯罪相比，身份盗用被视为是一项轻罪，身份窃贼很难被抓住。身份窃贼经常出现在许多不同的地点，执法官员有时往往认为身份盗用是别人的问题，身份盗用犯罪问题难以得到解决。一个评估报告称，在 700 个身份盗用案件中，不到一个犯罪分子被定罪量刑。可见，刑法对身份窃贼的震慑效果有限，况且刑法对受害者的救助也少得可怜<sup>⑥</sup>。

其二，侵权法保护说。针对个人信息，也有学者主张用侵权法来保护<sup>[4]</sup>。中国《侵权责任法》对个人信息保护虽然也有所规定，但该法第 36 条所规制的对象仅仅局限于网络用户和网络服务提供者。如同刑法救济一样，侵权责任法也属于事后救济，在互联网时代需要对网络安全以及个人信息进行全流程的监管才更为有效。当然，受害者可以寻求侵权法的救济，但起诉滥用个人信息的违法犯罪分子往往是徒劳。因为违法犯罪分子有时候很难被发现，即便被发现了，他们的经济条件也非常有限。受害者也可以起诉泄露该个人信息的公司或者起诉许可窃贼以受害人名义设立帐户的公司。虽然这种危害容易为人们所理解，但是法律必须确认公司违反了其最起码的注意义务以及由此引起的损害后果两者之间因果关系的存在，这些要素更加难以确定。法律通常将身份窃贼、黑客或者个人信息的滥用者视为首犯。数据被盗用的公司往往也被视为受害者，它们也因为身份被盗用而遭受损失。即便法律认定公司允许不正当获取个人信息主观上存在过错，进行法律诉讼仍存在一些障碍，很长一段时间之后才会发生实质性的损害，个人信息可能多年以后才被不当传播并用于身份盗窃。此外，也很难侦查身份窃贼是从何处获得个人信息并实施违法犯罪行为的。如

果一件有形财产被盗，它在某个时期只存在于某一个特定地方，信息则可以为不同的人同时拥有，而且可以进一步传播开来。除非我们能侦查到窃贼获取信息的源头，否则很难把具体损害与确保数据安全的特定实体两者联系起来<sup>⑦</sup>。

其三，隐私权客体说。该理论起源于美国，主张个人信息是一种隐私利益，个人信息立法应该采取隐私权保护模式。从形式逻辑出发，“个人信息”和“个人隐私”是包含关系，也就是说个人信息包含个人隐私，个人隐私是个人信息的下位概念，是个人信息的一部分。选择“个人隐私”的立法和观点主张法律保护个人信息是因为其涉及个人的隐私，换句话说，法律仅仅保护涉及个人隐私的个人信息，而不保护不涉及个人隐私的个人信息。而诸多个人信息并不涉及个人隐私，比如公开个人信息和琐碎个人信息，而这些个人信息仍然需要个人信息保护法给予保护。法律对个人信息的保护，是对满足一定条件的全部个人信息进行全面保护，并不只停留在保护隐私利益一个方面。个人信息保护法所保护的个人信息法律要件是该信息具有“识别性”，而不是具有隐私利益。因此，“个人隐私”这一概念事实上将不涉及隐私的个人信息排除在保护范围之外，显不足取<sup>[5]104-105</sup>。进而言之，个人信息权与隐私权是两个不同的权益范畴，两者具有不可调和性。信息权法规定，公民有权获取由政府机构拥有的个人信息。同时，隐私权法律规定，个人有权控制由政府 and 私人机构对其个人信息资料的收集、获取或者使用。隐私权和个人信息权通常被描述为“一枚硬币的两面”——主要是作为补充权利，即促进个人权利的自我保护和增强政府的责任。随着越来越多的国家进行相关的立法，隐私权法和个人信息权法之间的关系目前引起了全球范围内相当大的讨论。由于利益和价值的多元化需求，两者之间必然会存在某些交叉重叠，也不可避免会导致一些冲突。例如，政府有时候因为各种原因需要获取大量个人信息，记者进行新闻调查，民间社会团体为问责而斗争，个体需要知道政府部门做出某种决定的理由，公司为了营销目的而寻求信息，历史学家和学者则探究各种事件的来龙去脉等。对此，已有 50 多个国家分别颁布了

<sup>⑥</sup>Solove, Daniel J., *The New Vulnerability: Data Security and Personal Information* (August 9, 2011). SECURING PRIVACY IN THE INTERNET AGE, Radin & Chander, eds., Stanford University Press, 2008; GWU Law School Public Law Research Paper No. 102. Available at SSRN: <http://ssrn.com/abstract=583483>.

<sup>⑦</sup>Hon, W. Kuan, Millard, Christopher and Walden, Ian, *Who is Responsible for Personal Data in Cloud Computing? The Cloud of Unknowing, Part 2* (March 21, 2011). *International Data Privacy Law* (2012) 2 (1): 3-18; Queen Mary School of Law Legal Studies Research Paper No. 77/2011. Available at SSRN: <http://ssrn.com/abstract=1794130>.

隐私权法、数据保护法(data protection laws)和信息权法(RTI law)<sup>⑧</sup>。

其四,人格权客体说。该学说认为,个人信息体现的是一种人格利益,个人信息的保护应该采取人格权的保护模式。“人格权客体说”以德国法为代表。德国1990年修改后的个人资料法第一章《一般条款》第1条规定:“本法旨在保护个人的人格权,使其不因个人资料的处置而遭受侵害。该法的目的是为了保护个人人格权在个人信息处理时免受侵害。”从而放弃了原来作为舶来品的隐私权理论,转而寻求本国法律体系中比较完善的人格权理论。中国台湾资料法也采用“人格权客体说”。该法第1条规定:“为规范个人资料之搜集、处理及利用,以避免人格权受侵害,并促进个人资料之合理利用,特制定本法。”<sup>[5]119-120</sup>人格权法对个人信息权的保护,重点应确认个人对其享有的信息的权利范围、权利内容(如对个人信息资料的处分权、要求更正权、更新权、了解信息资料用途的权利);同时,应当规定有关收集利用信息资料的机构或个人的义务,如强调收集个人资料的主体的合法性、强调收集个人资料的目的的合法性、强调收集个人资料的手段的合法性、强调个人资料收集者的保密义务和忠实义务、强调尊重被收集者所享有的权利、未经被收集者的同意不得转让其个人资料等。从现代社会的发展对个人自由的扩展趋势而言,强化个人对其信息资料的积极控制,即“控制自己资讯的权利”或“资讯自决权”,有相当积极的作用,人格权法应予以积极地反映<sup>[6]</sup>。笔者认为,采用人格权的保护模式来保护个人信息无疑是正确的选择。但须注意的是,人格权与个人信息权亦是两个不同的权益范畴,两者既有交叉重叠的部分,也有不兼容之处。个人信息保护法的一半是民法,民法是调整平等主体之间财产关系和人身关系法律规范的总称。个人信息保护法的“一半”是调整横向的信息处理关系,且以个人信息为客体,而个人信息体现的是一种人格利益,属于人身利益的一种,这都说明个人信息保护法是民法的特别法。民法就全部承载有人格利益的私人信息给予保护,而个人信息保护法仅就符合个人信息保护法规定的“个人信息”提供保护。民法保护的是全部承载人格

利益的信息,笔者称为“私人信息”。私人信息是指一切可以识别自然人的信息。区分“个人信息”与“私人信息”不是文字游戏,而是十分必要。民法对私人信息的保护分别纳入人格权法的不同领域,如隐私、名誉等。而个人信息保护法仅保护形成记录的、储存于档案内的个人信息<sup>[5]182-182</sup>。

### 三、域外个人信息法律保护的立法例

就个人信息保护而言,目前存在美国的分散立法模式和欧盟的统一立法模式两种范例,这两种伦理框架在很大程度上明确了现代信息法的基本走向。必须指出的是,无论是基于效果论的立法体例还是自治论的立法体制,二者都是一把双刃剑。美国信息法的立足点是实用主义,强调的是信息的实用价值,它所采取的是分散立法和行业自律相结合的模式。就公共领域而言,为了规范联邦政府处理个人信息的行为,1974年颁行了《隐私法案》(Privacy Act),该法案适用于美国公民和在美国取得永久居留权的外国人。在私法领域,美国则采取了分散立法模式,主要依靠自律机制实现对个人信息的保护。而欧盟信息法则以道义论(deontological)作为其理论基础,该种立法体制侧重的是对个人信息提供保护,坚持个体自治的价值<sup>⑨</sup>。

1996年,欧盟通过了《数据保护指令》,从而在欧盟国家确立了隐私权立法的基本原则。正如乔尔·雷登堡(Joel Reidenberg)指出的,《数据保护指令》在其立法背景和基本理念上都异于美国。近年来,美国主要是通过市场而不是法律来解决隐私权的保护问题。与此相反,欧盟将隐私权视为基本的人权,因而政治上务必解决<sup>⑩</sup>。欧盟《数据保护指令》对个人信息提供了广泛的保护手段和救济措施,该综合性方法与美国形成了鲜明的对比,后者只在各种狭窄的范围内规范隐私权<sup>⑪</sup>。欧盟各国基本上都制定了全面的信息保护法,一并规范公私领域中的信息处理行为。

德国个人资料保护法(即《防止个人资料处理滥用法》)在大陆法系国家最具代表性,它采取统一立法模式,对个人资料保护进行统一规范、统一保护。1982年“人口普查法”违宪案成为德国个人资料保

⑧Burk, Dan L., Information Ethics and the Law of Data Representations. UC Irvine School of Law Research Paper No. 2008-5; Ethics and Information Technology, Vol. 10, pp. 135-147, 2008. Available at SSRN: <http://ssrn.com/abstract=1104466> or <http://dx.doi.org/10.2139/ssrn.1104466>.

⑨Joel R. Reidenberg, E-Commerce and Trans-Atlantic Privacy, 38 Hous. L. Rev. 717, 730 (2001).

⑩Solove, Daniel J., A Brief History of Information Privacy Law. PROSKAUER ON PRIVACY, PLI, 2006; GWU Law School Public Law Research Paper No. 215. Available at SSRN: <http://ssrn.com/abstract=914271>.

⑪参见中国台湾《个人资料保护法》第2条之规定。

护法发展的里程碑。之后,德国开始重新修订个人资料保护法,1990年颁布施行,该法获得了理论界和司法实务界的一致好评。首先,个人资料保护法确立了完备的原则体系。该法规定了直接原则、更正原则、目的明确原则、安全保护原则、公开原则、限制利用原则等。其次,个人资料保护法对监督机制作出了完整而系统的规定,设置了个人资料保护委员对公务机关处理个人资料的情况进行监督。同时还设置资料保护人对非公务机关处理个人资料进行监督。最后,个人资料保护法确立了损害赔偿制度。它是德国个人资料保护法的权利救济措施,也是信息主体补救权利的最终途径。德国个人资料保护法对个人资料的侵权行为分为行政侵权行为和民事侵权行为两大类。该法对于基于这两种侵权行为发生的损害赔偿进行了明确的区分和界定,分别规定了不同的归责原则和赔偿范围。对基于行政侵权行为发生的损害赔偿适用无过错责任原则,在赔偿范围的确定上,设定了明确的最高限额;而对民事侵权行为发生的损害赔偿则适用过错责任原则,在赔偿范围方面则实行全额赔偿,没有设定最高限额。

中国台湾地区早在1995年8月就颁布了“电脑处理个人资料保护法”,然而,由于该法保护客体过于狭隘、适用主体过于狭隘等客观原因,导致该法沉寂多年并未受到重视。鉴于最近几年陆续发生个人资料大量外泄事件,台湾执政当局和民众开始高度关切,经过多年努力,2010年4月27日终于通过新修订的《个人资料保护法》。新法的最大亮点有:其一,适用主体更具广泛性。旧“个资法”的适用主体仅为非公务机关。新法则规定,任何自然人、法人或其他团体,对个人资料的搜集、处理与利用原则上均受其调整。其二,扩大了保护客体。新法所保护的客体为所有个人资料,不再限于电脑处理的个人资料,人工处理的个人资料也包括在内。其三,行为规范更加合理。新法要求个人资料搜集者应于告知法定应告知事项后,取得个人资料本人所为允许之书面意思表示方属合法。甚且如系特定目的外利用个人资料需当事人书面同意者,不得以概括方式取得其同意,而应另以单独书面同意方式为之<sup>[7]</sup>。其四,新法强化了行政监管。一方面,为了强化对个人信息资料的保护,加重了目的事业主管机关的监管责任。另一方面,为了防止个人资料被滥用,新法明确规定了行政机关的检查事项及程序要求,从而规范了政府的行政行为。其五,规定了团体诉讼制度。为了鼓励民间公益团体能参与个人信息的保护,同时方便受害人更好地行使损害赔偿请求权,新

法规定了团体诉讼制度。须注意的是,台湾新个资法并不适用网络环境下的社交行为,而是适用民法的相关规定。

#### 四、中国个人信息法律保护的应然选择

个人信息保护问题本身跨越了宪法、行政法、民法和刑法等法律部门的界限,如果仅仅从某个部门法的角度观察它难免会顾此失彼。表面上看,信息法保护的是个人资料,但实质上,它不仅保护个人的隐私、自由和自治,事关个人人格的健全发展,它还具有重大的社会价值,关系到个人信息的公平、合理、高效流转。资料保护的个人和社会双重价值及资料保护问题的个人和社会双重属性,使资料保护法跨越了公法与私法的界限,涉足宪法、刑法、行政法和民法等部门法,任何一部传统的部门法单凭一己之力均无法完成个人信息法治化流转的使命。这就要求制定一部专门的资料保护法,使它成为规制个人资料收集、使用、加工和散播等整个信息流转过程的基础性法律。因此,中国亟需出台的不是针对某个领域、行业或某类资料处理的条例、管理办法、指导意见、行为守则,也不只是对刑法、行政法和民法中涉及资料保护的部分进行简单的修补,最亟需的是宪法指导下的一部个人资料保护法<sup>[8]</sup>。笔者认为,在借鉴域外成功立法经验的基础上,中国应该制定一部统一的“个人信息法”,确立个人信息保护的基本原则,明晰个人信息保护的各种法律关系,同时健全个人信息的救济措施和制度。

##### (一) 个人信息法基本原则的确立

个人信息法基本原则体现了信息法的基本价值,集中反映了信息法立法的宗旨和目的,对各项信息法律制度和信息法的规范起统帅和指导作用,也是指导我们立法、司法和实践活动的根本准则。一般认为,中国个人信息法应该确立以下几个基本原则:第一,信息收集限制原则。应该严格限制对个人信息的收集,所有的信息应该是通过合法正当的途径和手段获取的,而且信息主体应知情或者必须取得其同意。第二,信息质量原则。个人信息应该与其所使用的目的相关,而且在必要限度内,这些信息应该是准确、完整及最新的。第三,目的明确原则。个人信息收集的目的至迟在收集数据的当时应该明确,随后对信息的使用应仅限于实现该目的;每一次目的发生变化时,应进行具体说明,禁止超出该目的的范围收集和储存个人资料。第四,安全保障原则。个人信息应该处于安全保护中,避免可能发生的个人信息的泄露、意外灭失和不当使用。第五,公开原则。即个人信息的收集、利用与处理一般应当保持

公开,本人有权知悉个人信息的收集、利用和处理情况。第六,个人参与原则。为了保护个人信息的内容正确与完整,信息主体有权要求信息管理者确认是否获取了个人的相关信息,有权以合理的方式获得个人相应的信息,有权对相关的信息提出质疑,有权要求信息管理者纠正信息管理中的错误,也有权修改、完善或者删除个人相关信息<sup>②</sup>。第七,责任原则。信息管理者应该严格依法收集或使用个人信息,不能给信息主体造成任何伤害。否则,就要承担相应的法律责任。

### (二) 准确界定个人信息法律关系的主体制度

在个人信息保护法中,尽管法律关系主体包括自然人、国家机关、企事业单位、社会团体及其他非法人组织。但信息权利主体仅限于自然人,法人不能作为个人信息保护法律关系的权利主体。法人资料的功能和自然人不同,法人资料作为法人的一种信息资源,应该由其他法律加以保护,如民法、商业秘密保护法、反不正当竞争法等。从各国立法例看,大部分国家均采取这样的立场,认为个人信息保护法律关系的权利主体只限于自然人,对保护主体作为的是狭义的解释<sup>[9]</sup>。一般而言,信息主体就其个人信息资料而言依法享有查询或请求阅览,请求复制,请求补充或更正,请求停止搜集、处理或利用及请求删除等权利。

个人信息保护法律关系的义务主体一般分为两大类,即国家机关和非国家机关。国家机关是指从事国家管理和行使国家权力的机关,主要包括权力机关,行政机关和司法机关。国家机关一般是出于国家安全或者公共利益的需要而收集、处理和利用个人信息,但国家机关为履行职责而收集个人信息时应当在职权范围内进行,没有信息主体的书面同意,不得超越职权收集个人信息,不得侵害当事人的合法权益。政府机关在收集个人信息、建立个人信息数据库时,必须发布公告。政府机关必须保持个人信息的准确性、及时性和完整性,并保障信息的安全。

非国家机关是指国家机关以外的企业法人、非法人组织和其他自然人。非国家机关收集、处理和利用个人信息往往是出于商业目的,因此,对这类主体收集、处理和利用个人信息的条件应比国家机关更为严格。非国家机关未经登记管理机构进行业务资格登记并颁发执照的,不得收集个人信息。以个人信息收集或处理为主要业务的自然人、法人或其他信息处理主体,除非获得主管部门的批准并登

记管理机构进行业务资格登记并颁发执照,否则不得收集个人信息<sup>[10]</sup>。非国家机关搜集或处理个人信息必须符合以下条件:(1)法律明确规定;(2)与当事人有契约或类似契约关系的存在;(3)当事人自行公开或其他已合法公开的个人信息;(4)学术研究机构基于公共利益而进行统计或学术研究活动;(5)经当事人书面同意;(6)须与公共利益有关。

### (三) 明晰个人信息法律关系的客体制度及其对象

众所周知,民事法律关系的客体是指民事权利和民事义务所指向的对象。确切地说,民事法律关系的客体是指民事权利和民事义务所发生的事物。民事主体基于一定的对象而确定相互间的权利义务,没有客体,民事权利义务就会落空,也就不存在民事法律关系<sup>[11]</sup>。同理,信息法律关系的客体,是指信息主体所享有的民事权利和义务主体在收集、处理及利用个人信息过程中所应该承担的民事义务两者所共同指向的对象。由此可见,个人信息法律关系的客体指的是对个人信息的收集、处理及利用等行为。实践中,个人信息经常被滥用(abuse),从而发生身份盗用、诈骗、跟踪、滥用市场(例如垃圾邮件或电话推销)以及对信息主体进行监视等。这些滥用行为将会导致一些实质性伤害,例如经济损失、情绪困扰,甚至身体暴力等。身份盗用对于受害人而言简直就是一场梦魇。犯罪分子通过使用受害人的个人信息获得贷款,公开诈骗帐户,侵占受害人帐户中的财产。当身份盗用发生之后,受害者的个人档案因为错误信息而被玷污……因为犯罪分子盗用受害人的个人信息,导致执法数据库将受害者的名字与盗用者的犯罪活动联系起来<sup>[9]</sup>。可见,规范对个人信息的收集、处理及利用意义重大。

个人信息法律关系的对象是信息主体的个人信息。在个人信息的定义上,有概括型、概括列举型和识别型三种模式。概括型定义就是单独使用概括的方法描述个人信息的定义方式;列举型是单独使用列举的方法界定个人信息的定义模式。单独使用列举型定义的立法十分少见,而大部分采取混合型定义模式或者概括型定义模式。识别型模式就是以识别为核心要素对个人信息进行界定的定义方式。相比较而言,识别型定义是目前国际和国内立法采用较多的个人信息定义方式<sup>[5][10]</sup>。笔者认为,我们可以在参考《侵权责任法》第2条第2款立法模式的基础上采取识别型定义法,即中国《个人信息法》中所讲的个人信息——自然人姓名、出生年月日、身份证统

<sup>②</sup>参见《江苏省信息化条例》第43条之规定及《河北省信息化条例》第56条之规定。

一编号、护照号码、特征、指纹、婚姻、家庭、教育、职业、病历、医疗、基因、性生活、健康检查、犯罪前科、联络方式、财务情况、社会活动及其他得以直接或间接方式识别该个人的信息<sup>⑬</sup>。

#### (四) 构建健全的个人信 息权利救济和保护制度

与个人信息安全相关的核心问题是商业活动和政府行为。我们需要重构个人信息权与企业及政府的关系,也就是说,当企业及政府机构收集并利用个人信息时,他们怎样对待,这是我们需要严肃思考的问题。目前,个人信息的采集者和使用者往往对此不负责任。个人信息遭到收集和使用,然而信息主体根本就不知道也无 力掌控这些信息的安全性。对于收集和利用个人信息资料的公司企业须在多大程度上对信息主体承担责任,法律竟然没有明确规定<sup>[5]</sup>。个人信息权是一项重要的人权,建构健全的权利救济制度对信息主体至关重要。

笔者认为,应该从以下几个方面完善个人信息权利救济制度。(1)法律应该明确规定,国家机关和非国家机关在收集、处理或利用个人信息时,应当尊重当事人的合法权益,依诚实信用方法为之,不得逾越特定目的的必要范围,并应与收集的目的具有正当合理的关联。(2)归责原则的确定。一般认为,国家机关违反法律规定,导致个人资料遭不法搜集、处理、利用或者导致其他侵害行为发生的,须承担无过错责任原则。例如,德国《个人资料保护法》第7条规定:“当公务机关在本法或其他资料保护规定下,由于未经许可或不正确的个人资料自动化处理对资料本人造成损害的,公务机关有责任赔偿本人的损失,而不论其是否有过错。”对于非国家机关违反法律规定,导致个人资料遭不法搜集、处理、利用或者导致其他侵害行为发生,行为人不能证明自己没有过错的,应当承担侵权责任。进言之,非国家机关对其民事侵权行为导致损害后果发生的,应承担过错责任。例如,中国台湾《个人资料保护法》第29条规定:“非公务机关违反本法规定,致个人资料遭不法搜集、处理、利用或其他侵害当事人权利者,负损害赔偿责任。但能证明其无故意或过失者,不在此限。”(3)损害赔偿额的计算方法。鉴于个人信息上的侵害,往往难以计算具体的数额,因此,个人信息保护法往往通过定额赔偿制度来计算损害。但计算机处理个人信息的规模宏大,由于限定了最高额赔偿,可能使一些超过了最高额赔偿的损害无法得到

赔偿。在此情况下,应允许当事人依据民法主张赔偿全部损害。对于高出法定赔偿额的部分,当事人可以依据民法请求赔偿,当事人应该承担民法规定的证明责任<sup>[5]184</sup>。(4)行政责任及刑事责任的规定。笔者认为,中国个人信息法可以进行如下规定:任何单位和个人不得非法披露所采集的信息,不得将获取的公民、法人和其他组织的信息出售或以其他方式非法提供给他人,不得以窃取、购买等方式非法获取前述信息。违反法律规定非法披露、出售、提供信息,或者以窃取、购买等方式非法获取信息的,由国家行政主管部门责令其删除信息,没收违法所得,对单位处以10万元以上50万元以下罚款,对个人处以1万元以上5万元以下罚款;构成违反治安管理行为的,由公安机关依法给予治安管理处罚;构成犯罪的,依法追究刑事责任<sup>⑭</sup>。

#### 五、结语

个人信息法律保护有其深厚的伦理基础,包括隐私法和知识产权等在内的信息法很大程度上得益于一个连贯和全面的信息伦理理论。信息伦理理论的基石是信息实体(information entity)概念。原子世界充斥着信息、信息客体和信息实体,如果我们从网络的视角看,这个世界就是一个二进制世界(world of bits)。这样一种伦理原则体系显然对法律原理产生了相当大的影响。作为一套正式适用的道德规范,法律最终植根于一些框架性的指导原则,而信息伦理规范则提供了这样的原则。从广义上讲,信息伦理规范可能适用于法律的所有领域,适用于原子世界里有关管理和规范现实生活的所有规则。但在信息法领域和法律原则中,它越来越关注的是位(bits)而不是原子,信息伦理规范得到了直接的适用。正如信息伦理规范源于计算机伦理规范一样,将信息伦理规范适用于法律规范体系自然而然就形成了信息法的适用问题<sup>⑯</sup>。在当前个人信息法缺位的情形下,法院司法实践活动对保护信息主体的权益至关重要。理性通常允许采纳几个有效的解决方法,然而面对该问题的法官却必须设法用斩钉截铁的手段去解决这种棘手问题<sup>[12]</sup>。当然,司法并不是一项机械活动,法官也不是如自动售货机般的判决机器,输入法条和事实即可,法官适用法律,通常都需要解释法律,眼光需要在事实与规范之间流转往返,其中存在一定的能动空间。在依法独立审判的大原则下,法官应该在这个空间范围之内,运用法律

<sup>⑬</sup>参见中国台湾《个人资料保护法》第2条之规定。

<sup>⑭</sup>参见《江苏省信息化条例》第43条之规定及《河北省信息化条例》第56条之规定。

技术和法律思维,寻求个案的公正解决,努力取得法律效果和社会效果的统一<sup>[13]</sup>。

#### 参考文献:

- [1] 唐友伟. 个人金融信息保护工作亟待完善[J]. 金融会计, 2012(4):64-66.
- [2] 刘宪权,方晋晔. 个人信息权刑法保护的立法及完善[J]. 华东政法大学学报,2009(3):120-130.
- [3] 刘修军. 公民个人信息权的刑事保护刍论[J]. 青海社会科学,2009(6):173-176.
- [4] 罗海山,陈肖楠. 论个人信息的侵权法保护[J]. 海南师范大学学报:社会科学版,2012(1):38-41.
- [5] 齐爱民. 私法视野下的信息[M]. 重庆:重庆大学出版社, 2012.
- [6] 王利明. 人格权法制定中的几个问题[J]. 暨南学报:哲学社会科学版,2012(3):2-8.
- [7] 熊爱卿. 台湾个人资料保护法要述[J]. 山东科技大学学报:社会科学版,2011(2):59-66.
- [8] 孔令杰. 制定《个人资料保护法》的理论基础与立法构想[J]. 重庆社会科学,2009(9):96-99.
- [9] 张才琴,李晓秋. 论个人信息保护的法律关系[J]. 求实, 2009(s2):86-87.
- [10] 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[J]. 河北法学,2005(6):2-5.
- [11] 雷群安,肖少启,张小平. 民法总论[M]. 广州:广州出版社,2010:46.
- [12] E·博登海默. 法理学:法律哲学与法律方法[M]. 邓正来,译. 北京:中国政法大学出版社,2004:584.
- [13] 何勤华. 新形势下人民法院在提升法律体系的品质、维护法制权威的作用[J]. 法学,2011(8):17-20.

## The Path Analysis of Legal Protection on Personal Information

XIAO Shaoqi<sup>1,2</sup>

- (1. School of Law, Shaoguan University, Shaoguan 512005, P. R. China;  
2. School of Law, Chongqing University, Chongqing 400044, P. R. China)

**Abstract:** The right to personal information is a basic human right. Presently, legal protection to personal information in China far from satisfactory, particularly in cloud computing, personal information has been seriously misappropriated and abused. The issue of personal information protection covers and even exceeds the boundaries of different legal departments such as the constitution, administrative law, criminal law and civil law etc. If observed just from a branch law perspective, it is probable that we would attend to one thing and lose the sight of another. As a consequence, we should formulate a consolidated statute to protect our personal information, in which we are supposed to establish the scientific principles, define accurately the subject system as well as elaborate clearly the object system and its pointed objects in the personal information legal relationship, and simultaneously construct reasonable right relief systems to personal information.

**Key words:** personal information; right to personal information; legal protection; legislation.

(责任编辑 胡志平)