个人信息保护研究丛书之三

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

周汉华 著

Personal Information Protection Act (Experts on) and the Legislative Study

法律出版社
LAW PRESS·CHINA

图书在版编目(CIP)数据

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/周汉华著.
—北京:法律出版社,2006.9
(个人信息保护研究丛书)
ISBN 7-5036-6646-3

Ⅰ.中… Ⅱ.周… Ⅲ.个人信息保护法—立法—研究报告—中国 Ⅳ.D923.04

中国版本图书馆 CIP 数据核字(2006)第 107681 号

个人信息保护研究丛书之三 | **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** | 周汉华 著 | 责任编辑 王旭坤 龚 瑜 装帧设计 汪奇峰

开本 A5　　**印张** 3.5　　**字数** 77 千
版本 2006 年 9 月第 1 版　　**印次** 2006 年 9 月第 1 次印刷
出版 法律出版社　　**编辑统筹** 法学学术出版分社
总发行 中国法律图书有限公司　　**经销** 新华书店
印刷 北京北苑印刷有限责任公司　　**责任印制** 陶 松

法律出版社/北京市丰台区莲花池西里 7 号(100073)
电子邮件/info@lawpress.com.cn　　销售热线/010-63939792/9779
网址/www.lawpress.com.cn　　咨询电话/010-63939796

中国法律图书有限公司/北京市丰台区莲花池西里 7 号(100073)
全国各地中法图分、子公司电话:
第一法律书店/010-63939781/9782　　西安分公司/029-85388843
重庆公司/023-65382816/2908　　上海公司/021-62071010/1636
北京分公司/010-62534456　　深圳公司/0755-83072995
苏州公司/0512-65193110

书号:ISBN 7-5036-6646-3/D·6363　　**定价**:11.00 元

目录
MULU

中华人民共和国个人信息保护法

ZHONGHUARENMINGONGHEGUOGERENXINXIBAOHUFA

(专家建议稿)

第一章　总则

[立法目的与依据]

第一条　为规范政府机关或其他个人信息处理者对个人信息的处理,保护个人权利,促进个人信息的有序流动,根据宪法制定本法。

[合法原则]

第二条　政府机关或其他个人信息处理者对个人信息的处理,应符合本法的规定,法律另有明确规定的除外。

[权利保护原则]

第三条　信息主体有权要求政府机关或其他个人信息处理者公开其所掌握的关于本人的个人信息。

信息主体发现个人信息记录的内容有错误或不准确的,可以要求政府机关或其他个人信息处理者予以更正或者停止使用。

[利益平衡原则]

第四条　对个人信息的保护,不得妨碍他人的权利与

自由,不得损害国家利益与社会公共利益。

[信息质量原则]

第五条　政府机关或其他个人信息处理者应采取措施,保证个人信息仅用于与收集目的相关的领域,并保证个人信息的准确性、完整性和及时性。

[信息安全原则]

第六条　政府机关或其他个人信息处理者应采取必要的保护措施,防止个人信息的泄露、丢失、毁损或其他安全事故。

[职业义务原则]

第七条　政府机关或其他个人信息处理者的工作人员对任职期间因处理个人信息所获知的内容,负有保守秘密的职业义务,不得擅自告知他人或者以其他方式加以披露或使用。

[救济原则]

第八条　信息主体认为政府机关或其他个人信息处理者的信息处理违反本法,侵犯其合法权益的,有权依法请求行政救济或提起诉讼。

政府机关或其他个人信息处理者的违法行为给信息主体的合法权益造成损害的,应依法承担赔偿责任。

公民、法人或者其他组织认为政府信息资源主管部门的具体行政行为侵犯其合法权益的,有权依法申请行政复议或提起行政诉讼。

[适用范围]

第九条　本法适用于政府机关或其他个人信息处理者对个人信息的处理。除本法另有明确规定外：

“政府机关”指行政机关与法律、法规授权行使行政管理职能或提供公共服务的其他组织。

“其他个人信息处理者”指政府机关之外，依据本法规定进行个人信息处理的法人、组织或个人。

“个人信息”指个人姓名、住址、出生日期、身份证号码、医疗记录、人事记录、照片等单独或与其他信息对照可以识别特定的个人的信息。

“个人信息文件”指存储于计算机或其他媒介之上，依据一定的标准或方法，可以检索个人信息的文件。

“处理”指政府机关或其他个人信息处理者根据一定的编排标准或检索方式，以自动或非自动方法对个人信息的收集、存储、使用、交换、公开、修改、删除、销毁等行为。

“信息主体”指通过个人信息可以被识别出来的特定个人。

[适用例外]

第十条　本法的规定不适用于国家安全机关为保障国家安全而进行的个人信息处理。

本法的规定不适用于公民在纯粹的个人或家庭活动中所进行的个人信息处理。

法人或其他组织所处理的个人信息数量较少，处理活动不太可能对个人权利造成侵害的，不适用本法。

第一款规定的范围由国务院确定。

第三款规定的范围由国务院信息资源主管部门通过制定规章确定。

第二章　政府机关的个人信息处理

第一节　个人信息的收集与使用

[明确使用目的]

第十一条　政府机关只能在其法定职权范围内,为履行其职责收集个人信息。

政府机关收集个人信息,必须有明确、合法和特定的使用目的。

政府机关收集个人信息,不得超出实现第二款所规定的使用目的的范围。

政府机关收集个人信息应尽可能减轻社会负担,避免重复收集个人信息,并应当及时删除与其处理目的无关的信息。

[登记程序]

第十二条　政府机关开始收集个人信息之前,应就下述事项向各级人民政府信息资源主管部门进行登记:

(一)个人信息文件的名称;

(二)个人信息的使用目的;

(三)收集机关的名称;

(四)个人信息的主要内容;

(五)个人信息的收集方法;

(六)个人信息的保存期限;

(七)个人信息文件的主要使用者;

(八)个人信息文件的公开方式与地点;

(九)其他事项。

个人信息有以下情形之一的,不适用第一款的规定:

(一)涉及国家安全、国家秘密以及其他重大国家利益的事项;

(二)涉及犯罪预防、刑事侦查、公诉、审判与执行刑罚的事项;

(三)涉及行政处罚与行政强制执行的事项;

(四)涉及出入境管理的事项;

(五)涉及税收征管的事项;

(六)涉及政府机关内部人事管理的事项;

(七)政府机关为处理内部业务而使用的个人信息文件;

(八)政府机关为进行计算机的试验性操作而使用的个人信息文件;

(九)法律、法规所规定的其他事项。

[登记事项公告]

第十三条　政府信息资源主管部门完成第十二条第一款所规定的登记程序后三十日内,应通过政府公报或其他方式,将登记信息予以公告。

[制作个人信息文件登记簿]

第十四条　政府机关应根据其持有的不同的个人信息文件,分别制作记录第十二条第一款所规定事项的个人信息文件登记簿,供公众查阅。

[使用限制]

第十五条　政府机关只能在收集个人信息时所明确

的使用目的范围内处理个人信息。

符合以下条件之一的,政府机关可以在使用目的范围之外处理个人信息:

(一)信息主体同意或者向信息主体提供;

(二)履行政府机关法定职责必须使用该个人信息;

(三)为维护国家安全或其他公共利益;

(四)为履行国际法义务提供给外国政府或者国际组织;

(五)有利于信息主体的合法权益;

(六)有利于防止他人重大权益受到损害;

(七)以不能识别特定个人的形式,供学术研究或统计之用;

(八)有正当理由并且仅供政府机关内部使用;

(九)法律、法规规定的其他情况。

政府机关将第二款所规定的个人信息提供给信息主体之外的第三人的,应当同时就使用目的、使用方法、再交换条件以及其他重要事项,做出明确的限制。接收个人信息的第三人必须遵守这些限制条件。

政府机关认为对于保护个人权利和利益有必要的,可以将在使用目的之外处理个人信息的主体限定于该机关内的特定部门。

第二节　信息主体获得个人信息的权利

[获得个人信息的权利]

第十六条　信息主体有权要求政府机关公开其所持有的关于本人的个人信息。

[申请的程序]

第十七条　申请人申请公开个人信息应当递交申请书,申请书应当载明下列事项:

(一)申请人的姓名、身份证号码、住址;

(二)申请人的联系方式;

(三)所要公开的个人信息的描述,申请人的描述应足以使政府机关识别所要申请的个人信息;

(四)提出申请的时间。

申请人递交申请书时,应当一并提交证明其为所申请的个人信息本人的文件。

申请书既可以在政府机关办公地点提出,也可以采用挂号邮寄、传真、电子邮件的方式提出。

申请书在受理机关办公地提出的,受理机关应当场登记,并给申请人出具回执。申请书以挂号邮寄、传真、电子邮件方式提出的,受理机关应当在收到后当天登记。

[政府机关的帮助]

第十八条　政府机关应当为公众申请获得个人信息提供帮助。

根据本法第十七条递交的申请书所记载的事项不完备的,政府机关应给予其机会补正、更正。

[政府机关的公开义务与例外]

第十九条　申请人提出公开请求的,政府机关有义务向申请人公开其个人信息。

符合以下条件之一的个人信息,作为例外不予公开:

(一)本法第十二条第二款所规定的信息;

(二)有可能对申请人的生命、健康、生活或者财产造成危害的信息;

(三)有可能对第三人利益造成损害的信息;

(四)有可能影响政府机关查处违法行为的执法活动的信息。

[利益平衡或损害衡量原则]

第二十条　对于不应公开的个人信息,政府机关如果认为有明显的公共利益需要要求公开的,或者公开不会造成实质性损害,或者公开对于保障个人的权利极为必要的,可以决定予以公开。

[信息的可分割性]

第二十一条　尽管被申请的个人信息包含有不予公开的内容,但如果能够将不予公开的内容与可以公开的内容区别开,政府机关应向申请人提供可以公开部分的个人信息。

[拒绝回答个人信息是否存在]

第二十二条　对于不予公开的个人信息,如果回答其存在便会导致该信息被公开的后果的,政府机关可以不明确回答该个人信息是否存在。

[书面告知决定]

第二十三条　有下列情形的,政府机关应当自登记之日起十日内书面告知申请人:

(一)申请的个人信息不存在;

(二)政府机关已采取所有必要措施,仍无法查找到申请的个人信息;

(三)政府机关虽然不拥有申请的个人信息,但知道该信息由其他政府机关拥有的,告知申请人向其他政府机关提出申请;

(四)有本法第二十二条规定的情形,不确认申请的个人信息是否存在。

[正式决定]

第二十四条　政府机关应当自登记之日起十五日内,根据不同情况,分别做出以下决定:

(一)申请符合本法应当予以公开的规定,做出准予公开个人信息的决定;

(二)具有本法第二十一条规定的情形,做出准予部分公开个人信息的决定;

(三)具有本法第十九条第二款规定的情形,做出不准公开个人信息的决定。

超出第一款规定的期限,政府机关没有做出正式决定的,视为决定不予公开。

[正式决定的内容]

第二十五条　政府机关依照本法第二十四条第一款第(一)项做出准予公开个人信息决定的,应书面告知申请人获得个人信息的时间、地点、形式、应支付的费用。

政府机关依照本法第二十四条第一款第(二)项、第(三)项做出准予部分公开或不准公开个人信息决定的,应该制作决定书,并依法送达申请人。决定书应当说明拒绝的理由、法律依据、救济途径和期限。

[获得个人信息的形式]

第二十六条　政府机关可以以下列方式向申请人公开个人信息:

(一)个人信息以文书、图片、照片等形式存在的,向申请人提供复印件,或者安排申请人查阅。

(二)个人信息以胶卷、磁带、软盘、视听资料等可复制的方式存在的,可以安排申请人观看,也可以向申请人提供该信息内容的书面记录。政府机关利用自身的一般设备就能复制该内容的,如果申请人要求,应当向申请人提供复制副本。

(三)个人信息以计算机读取的形式存在的,可以向申请人提供磁盘复制件,或者向申请人提供打印记录。

视力、听力或者语言有缺陷的人有权申请以与其能力相符合的特殊形式获得个人信息。

[成本收费标准]

第二十七条　申请人申请获得个人信息应支付检索费、复制费、邮寄费。政府机关收取的费用不得超出因提供个人信息发生的实际成本,收取标准由省级价格、财政主管部门统一确定。

申请人应当先缴纳费用,凭支付凭证获得个人信息。

申请人确有经济上困难的,经政府机关负责人批准,可以少交或免交本条第一款规定的费用:

第三节　个人信息的更正与停止使用

[更正与停止使用请求权]

第二十八条　根据本法第十六条获得个人信息的信息主体发现个人信息记录的内容有错误或不准确的,可以请求政府机关予以更正或者停止使用。

[政府机关的更正与停止使用义务]

第二十九条　政府机关收到申请人的申请后,经查证确认申请人的申请成立的,有义务更正或者停止使用相关的个人信息。

[申请人的查证协助]

第三十条　申请人可以在递交更正或者停止使用个人信息申请的同时或者之后,向政府机关提供有关证明资料,协助政府机关查证事实。

政府机关在查证过程中,可以要求申请人或第三人提供有关证明资料,协助查证。

[正式决定]

第三十一条　政府机关应当自收到申请人的申请之日起十五日内,根据不同情况,分别做出以下决定:

(一)申请成立的,做出更正或者停止使用个人信息的决定;

(二)申请不成立的,做出不予更正或者停止使用个人信息的决定;

(三)申请的事项复杂,有正当理由无法在规定的时限内完成的,经政府机关领导人批准,可以延长十五日作出决定;

申请的事项特别复杂,根据第一款第(三)项的规定延长期限后仍无法作出决定的,经政府机关领导人批准,可以再次延长作出决定的期限,但最长不得超过三十日。

[正式决定的内容]

第三十二条　政府机关依照本法第三十一条第一款第(一)项做出更正或停止使用个人信息决定的,应书面告知申请人决定的具体内容。

政府机关依照本法第三十一条第一款第(二)项做出不予更正或者停止使用个人信息决定的,应该制作决定书。决定书应当说明拒绝的理由、法律依据、救济途径和期限。

政府机关依照本法第三十一条第一款第(三)项、第二款做出延期决定的,应书面告知申请人延长的期限以及延长的理由。

[更正或停止使用决定的通知]

第三十三条　政府机关依照本法第三十一条第一款第(一)项做出更正或停止使用个人信息的决定后,可依职权或信息主体的申请,以书面形式,向曾经接收该个人信息的第三人发出通知,告知决定的内容。

[程序的准用]

第三十四条　除本节另有规定外,申请人请求更正或者停止使用个人信息适用本章第二节规定的程序。

第三章　其他个人信息处理者的个人信息处理

第一节　政府管理制度

[登记与行政许可]

第三十五条　其他个人信息处理者开始进行个人信息收集之前,须向政府信息资源主管部门进行登记。

以个人信息处理为主要业务或通过个人信息处理营利的公民、法人或其他组织,在开始进行个人信息收集之前,须经政府信息资源主管部门行政许可。

除本法另有规定外,本章规定的行政许可适用《中华人民共和国行政许可法》的规定。

[登记与行政许可申请事项]

第三十六条　进行登记或申请行政许可,应向政府信息资源主管部门递交申请书。申请书应当载明下列事项:

(一)自然人的姓名、身份证号码、住址,法人或者其他组织的名称、住所、法定代表人或主要负责人的姓名;

(二)个人信息文件的名称;

(三)个人信息的使用目的;

(四)个人信息的主要内容;

(五)个人信息的收集方法;

(六)个人信息的保存期限;

(七)个人信息文件的主要使用者;

(八)个人信息文件的公开方式与地点;

(九)个人信息文件的安全保护措施;

(十)个人信息文件安全保护主要负责人姓名、身份证号码、住址及简历;

(十一)国务院信息资源主管部门要求的其他事项。

[审查程度]

第三十七条　除特殊情况外,政府信息资源主管部门对登记事项原则上只进行形式审查。

政府信息资源主管部门对行政许可事项除了进行形式审查之外,还须进行实质审查。

[正式决定]

第三十八条　政府信息资源主管部门应当自收到申请之日起十五日内,根据不同情况,分别做出以下决定:

(一)登记或行政许可申请符合法定条件、标准的,做出准予登记或行政许可的书面决定;

(二)登记或行政许可申请不符合法定条件、标准,或者个人信息处理极有可能对个人权利造成实质性危害的,做出不予登记或行政许可的书面决定。

政府信息资源主管部门做出第一款第(二)项不予登记或行政许可的决定的,应当说明理由,并告知申请人享有依法申请行政复议或者提起行政诉讼的权利。

[决定的公告]

第三十九条　政府信息资源主管部门做出登记或行政许可决定后三十日内,应通过政府公报或其他方式,将

决定内容予以公告,供公众查阅。

其他个人信息处理者被准予登记或行政许可后,应将本法第三十六条规定的事项制作个人信息文件登记簿,供公众查阅。

[变更手续]

第四十条　本法第三十六条第一款规定的事项发生变更的,其他个人信息处理者应于变更事由发生之日起十日内,申请政府信息资源主管部门办理变更手续。

[注销登记]

第四十一条　其他个人信息处理者终止进行个人信息处理活动的,应于终止之日起十日内,申请政府信息资源主管部门办理注销登记。

其他个人信息处理者终止进行个人信息处理活动的,应销毁其所拥有的个人信息文件,或经政府信息资源主管部门同意后做其他处置。

[不收费]

第四十二条　政府信息资源主管部门办理登记或行政许可事宜,不得收取任何费用。

第二节　个人信息的收集与使用

[个人信息处理的合法性标准]

第四十三条　除满足下述条件之一的以外,其他个人

信息处理者不得进行个人信息处理:

(一)信息主体明确同意;

(二)与信息主体存在合同关系或类似关系,为完成合同义务必须进行个人信息处理;

(三)个人信息处理有利于保护信息主体的重要利益;

(四)个人信息处理有利于保护第三人的合法权益;

(五)个人信息处理有利于保护公共利益;

(六)法律、法规规定的其他情形。

[特定的使用目的]

第四十四条　其他个人信息处理者收集或处理个人信息必须有明确、特定的使用目的。

[使用目的限制]

第四十五条　其他个人信息处理者超出本法第四十四条所规定的使用目的处理个人信息的,必须经信息主体事先同意。

符合以下条件之一的,其他个人信息处理者可以不经信息主体的事先同意,超出本法第四十四条所规定的使用目的处理个人信息:

(一)法律、法规有明确规定;

(二)对于保护人的生命、身体或者财产极为必要但又很难得到信息主体同意;

(三)对于国家机关履行法定职责极为必要,且征得信息主体的同意会妨碍国家机关履行其法定职责。

[正当收集个人信息]

第四十六条　其他个人信息处理者必须通过合法、正

当方式收集个人信息。

[直接收集时对信息主体的告知]

第四十七条　其他个人信息处理者直接自信息主体收集其个人信息时,应将下述事项告知信息主体:

(一)其他个人信息处理者的身份;

(二)个人信息的使用目的;

(三)个人信息文件的主要使用者;

(四)个人信息文件的公开方式与地点;

(五)其他对信息主体权利可能造成重大影响的事项。

[跨境信息传输的特别规定]

第四十八条　符合下述条件之一的,政府信息资源主管部门可以限制其他个人信息处理者进行跨境个人信息传输:

(一)涉及国家安全与其他重大国家利益;

(二)中国政府承担的国际法义务有特别要求;

(三)接收个人信息的国家或地区不能对个人信息提供充分的法律保护;

(四)法律规定的其他情形。

国务院信息资源主管部门负责认定第一款第(三)项所规定的国家或地区,并规定认定的具体标准、方法和程序。

第三节　信息主体的权利

[获得个人信息的权利]

第四十九条　信息主体请求获得个人信息的,其他个

人信息处理者应尽快予以提供。

有下述情况之一的,其他个人信息处理者对个人信息的全部或部分可以不予提供:

(一)有可能对信息主体的生命、健康、生活或者财产造成危害的信息;

(二)有可能对第三人利益造成损害的信息;

(三)信息主体对相同个人信息文件反复提出公开请求,明显对其他个人信息处理者的正常个人信息处理工作造成妨碍的;

(四)法律、法规规定的其他情况。

[更正与停止使用请求权]

第五十条　根据本法第四十九条获得个人信息的信息主体发现个人信息记录的内容有错误或不准确的,可以要求其他个人信息处理者予以更正或者停止使用。

其他个人信息处理者经查证确认信息主体的请求成立的,应尽快更正或者停止使用相关个人信息。

其他个人信息处理者经查证认定信息主体的请求不成立的,可以拒绝更正或者停止使用相关个人信息。

[说明理由]

第五十一条　其他个人信息处理者根据本法第四十九条第二款、第五十条第三款的规定,做出不予提供全部或部分个人信息、拒绝更正或者停止使用个人信息的决定,应以书面形式向信息主体说明理由。

[收费标准]

第五十二条　信息主体根据本法第四十九条获得个

人信息的,应向其他个人信息处理者支付成本费用。

第一款所规定的成本费用标准,由各地方政府物价管理部门确定。

第四节　行业自律机制

[行业自律组织]

第五十三条　国家鼓励其他个人信息处理者在自愿的基础上成立行业自律组织,并创造条件,逐步向行业自律组织转移政府职能。

行业自律组织的设立条件和要求,由国务院信息资源主管部门具体规定。

行业自律组织成立后,应在政府信息资源主管部门进行登记,接受政府信息资源主管部门的指导和监督。

[行业自律组织的职能]

第五十四条　行业自律组织履行下述职能:

(一)制定本行业的行为准则;

(二)推广本行业的执业可信度认证标志;

(三)协调本行业与政府信息资源主管部门的关系;

(四)接受信息主体的投诉,对信息主体与成员之间的争议进行协调、处理;

(五)处理行业自律组织成员之间的关系;

(六)行业自律组织章程规定的其他职能;

(七)政府信息资源主管部门委托的其他职能。

行业自律组织的章程应报政府信息资源主管部门备案。

第四章　法律的实施保障与救济

[信息资源主管部门]

第五十五条　县级以上人民政府信息资源主管部门负责组织、指导、推动、监督本法的实施。

[复议前置]

第五十六条　信息主体认为政府机关就个人信息公开、更正或停止使用的决定违反本法,侵犯其合法权益的,应首先向同级人民政府信息资源主管部门申请行政复议。

[复议案件决定机制与信息委员会]

第五十七条　政府信息资源主管部门根据行政复议法的规定,受理行政复议申请,做出行政复议决定。

有条件的地方,政府信息资源主管部门可以吸收本部门之外的专家,组建独立的信息委员会,受理行政复议申请,做出行政复议决定,行使其他行政管理权力。

信息委员会为非常设机构,其日常联络机构为各级人民政府的信息资源主管部门。

根据第二款的方式做出行政复议决定的,专家委员的人数应占信息委员会委员总数的三分之一以上。

[行政诉讼]

第五十八条　信息主体不服行政复议决定的,可以依

法向人民法院提起行政诉讼。

[投诉处理]

第五十九条　政府机关或其他个人信息处理者应建立有效的投诉处理机制,迅速处理信息主体提出的各种投诉。

[行业自律机制]

第六十条　信息主体认为其他个人信息处理者的个人信息处理行为违反本法的规定,侵犯其合法权益的,可以向其他个人信息处理者所属的行业自律组织提出投诉。

行业自律组织接受信息主体的投诉后,应公正、迅速地进行处理,提出处理意见或建议。

对于拒不接受行业自律组织处理意见或建议的成员,行业自律组织可以根据其章程的规定,做出撤销其执业可信度认证标志、中止其成员资格等进一步处理决定。

[行政措施]

第六十一条　信息主体认为其他个人信息处理者的个人信息处理行为违反本法的规定,侵犯其合法权益的,可以向政府信息资源主管部门举报,请求政府信息资源主管部门保护其合法权益。

政府信息资源主管部门可以根据信息主体的举报或者依职权,对其他个人信息处理者进行现场检查,要求提供信息处理情况报告,采取查封、扣押、冻结等行政强制措施。

进行现场检查,应当经政府信息资源主管部门负责人批准。现场检查时,检查人员不得少于二人,并应当出示

合法证件和检查通知书;检查人员少于二人或者未出示合法证件和检查通知书的,其他个人信息处理者有权拒绝检查。

[行政决定]

第六十二条　其他个人信息处理者违反本法规定进行个人信息处理的,政府信息资源主管部门应当责令限期改正;逾期未改的,或者其行为严重侵犯信息主体合法权益的,根据不同情况,政府信息资源主管部门可以做出如下决定:

(一)责令暂停个人信息处理;

(二)责令消除影响,赔礼道歉;

(三)责令停止使用个人信息文件;

(四)责令销毁个人信息文件;

(五)罚款;

(六)吊销个人信息处理登记证或许可证。

[司法救济]

第六十三条　信息主体认为其他个人信息处理者的个人信息处理行为违反本法的规定,侵犯其合法权益的,可以依法直接向人民法院提起民事诉讼,要求停止侵害,消除影响。

[赔偿责任与赔偿诉讼]

第六十四条　政府机关或其他个人信息处理者的信息处理行为违反本法的规定,给信息主体的合法权益造成损害的,应依法承担赔偿责任。

信息主体既可以向政府机关或其他个人信息处理者

请求赔偿,也可以直接依法向人民法院提起诉讼。

第五章　法律责任

[主管部门工作人员的责任]

第六十五条　政府信息资源主管部门的工作人员有下列情形之一的,依法给予行政处分;构成犯罪的,依法追究刑事责任:

(一)对符合法定条件的个人信息处理登记或行政许可申请不予准许的;

(二)对不符合法定条件的个人信息处理登记或行政许可申请准予登记或许可的;

(三)不在规定期限内将个人信息处理登记或许可事项予以公告的;

(四)办理登记或行政许可事宜收费或变相收取费用的;

(五)违反规定进行现场检查的;

(六)违反规定对其他个人信息处理者采取措施或处罚的;

(七)对信息主体的举报故意压制或不履行法定职责的;

(八)滥用职权、玩忽职守的其他行为。

政府信息资源主管部门的工作人员贪污受贿、泄露国家秘密或者所知悉的商业秘密,构成犯罪的,依法追究刑事责任;尚不构成犯罪的,依法给予行政处分。

[未经登记、许可处理个人信息的法律责任]

第六十六条　公民、法人或者其他组织未经登记或行

政许可,擅自处理个人信息的,由政府信息资源主管部门予以取缔;构成犯罪的,依法追究刑事责任;尚不构成犯罪的,由政府信息资源主管部门没收违法所得,违法所得五万元以上的,并处违法所得一倍以上五倍以下罚款;没有违法所得或违法所得不足五万元的,处一万元以上十万元以下罚款。

[政府机关违法处理个人信息的责任]

第六十七条　政府机关有下列情形之一的,由政府信息资源主管部门责令改正;情节特别严重或者逾期不改正的,对直接责任人和相关负责人依法给予行政处分;构成犯罪的,依法追究刑事责任:

(一)不能及时采取措施以保证个人信息的准确性、完整性和及时性的;

(二)由于安全措施不到位,导致个人信息的泄露、丢失、毁损或其他安全事故的;

(三)不按照规定办理登记或许可事项的;

(四)不制作个人信息文件登记簿供公众查阅的;

(五)超出使用目的范围收集信息的;

(六)不符合法定条件,超出使用目的处理个人信息的;

(七)不公开应该公开的信息的;

(八)不更正或停止使用应该予以更正或停止使用的个人信息的;

(九)超出收费标准收费的。

[其他个人信息处理者违法处理个人信息的责任]

第六十八条　其他个人信息处理者有下列情形之一的,由政府信息资源主管部门责令改正,处五千元以上五

万元以下罚款,有违法所得的,没收违法所得;情节特别严重或者逾期不改正的,处五万元以上十万元以下罚款,可以责令暂停个人信息处理或者吊销个人信息登记证或许可证;构成犯罪的,依法追究刑事责任:

(一)不能及时采取措施以保证个人信息的准确性、完整性和及时性的;

(二)由于安全措施不到位,导致个人信息的泄露、丢失、毁损或其他安全事故的;

(三)不按照规定办理登记或许可事项的;

(四)不制作个人信息文件登记簿供公众查阅的;

(五)违反合法性标准处理个人信息的;

(六)以不正当方式收集个人信息的;

(七)直接自信息主体处收集信息,不告知相关事项的;

(八)不符合法定条件,超出使用目的处理个人信息的;

(九)违反规定,进行跨境信息传输的;

(十)不公开应该公开的信息的;

(十一)不更正或停止使用应该予以更正或停止使用的个人信息的;

(十二)超出收费标准收费的。

[违反职业义务的责任]

第六十九条　政府机关工作人员擅自告知他人或者以其他方式披露任职期间因处理个人信息所获知的内容的,依法给予行政处分;构成犯罪的,依法追究刑事责任。

其他个人信息处理者的工作人员擅自告知他人或者以其他方式披露任职期间因处理个人信息所获知的内容的,有违法所得的,没收违法所得,违法所得五千元以上的,并处违法所得一倍以上五倍以下罚款;没有违法所得

或者违法所得不足五千元的,处一千元以上二万元以下罚款;构成犯罪的,依法追究刑事责任。

政府机关工作人员终止公务员身份以后有第一款规定行为的,根据第二款的规定追究责任。

[行业自律组织的责任]

第七十条　行业自律组织有下列情形之一的,由政府信息资源主管部门责令改正,处一千元以上五千元以下的罚款;情节严重或者逾期不改正的,处五千元以上五万元以下罚款:

(一)违反国务院信息资源主管部门规定的条件和要求,设立行业自律组织的;

(二)行业自律组织成立后,不在政府信息资源主管部门进行登记的;

(三)行业自律组织的章程不报政府信息资源主管部门备案的。

第六章　附则

[实施细则]

第七十一条　国务院信息资源主管部门可以根据本法制定有关具体实施办法。

[施行日期]

第七十二条　本法自_____年_____月_____日起施行。

本法施行之前已经进行个人信息处理的政府机关或其他个人信息处理者,必须在本法施行之日起半年内根据本法的规定加以规范,补办手续。

《个人信息保护法》(专家建议稿)
GERENXINXIBAOHUFA ZHUANJIAJIANYIGAO
立法研究报告

第一,关于法律的名称[①]

据我们不完全统计,世界上制定了个人信息保护法律的国家或地区已经超过五十个。就法律名称使用的概念而言,主要有三个,分别是"个人数据"、"个人信息"与"隐私"。其中,使用个人数据概念的国家或地区最多,主要是欧洲理事会、欧盟、欧盟成员国以及其他受欧盟 1995 年指令影响而立法的其他大多数国家。在普通法国家(英国作为欧盟成员国除外),如美国、澳大利亚、新西兰、加拿大,以及受美国影响较大的 APEC,则大多使用隐私概念。[②]在日本、韩国、俄罗斯等国,则使用个人信息概念。除了这三个概念之外,还有诸如"个人生活保护法"(智利)这样的概念。有时,还会同时并行使用个人数据与隐私(经济合作与发展组织 1980 年指南),隐私与个人信息(加拿大既有隐私法,又有个人信息保护与电子文件法),或者个人信息与个人数据(日本个人信息保护法中既有个人信息概念,也有个人数据概念)。

概念的不同主要是源于不同的法律传统和使用习惯,实质上并不影响法律的内容。[③]就内容而言,各国或地区的个人信息保护法虽然在许多方面具有重大的差别,但是,它们都具有如下两个共同的特征:第一,法律保护的对象是作为自然人的个人,而不是企业或其他组织。[④]第二,法律所要实现的目标是使能够识别特定个人的信息不被随意收集、传播或作其他处理,侵犯个人的权利。因此,法

① 对个人信息加以保护源于古老的隐私权。在人类各主要法律文明中,承认人们的隐私权利历史久远。可兰经、圣经以及犹太法中都大量地提到隐私权,古希腊与中国也有对隐私的保护("非礼勿听、非礼勿视、非礼勿言")。对隐私的法律保护在西方国家有几百年的历史。1361 年,英格兰治安法官法规定对偷窥者和偷听者加以逮捕。国会党人 William Pitt(1763 年)写下了著名的"风能进,雷能进,雨能进,国王不能进"的名言,表明了个人对其隐私的绝对权利。随后,各国对隐私权的法律保护逐步得以发展。1776 年,瑞典国会制定公共档案获取法,要求所有的政府信息只能用于合法的目的。法国于 1858 年禁止公开私人的事实并对违反者施以严厉的罚金。1889 年的挪威刑法典禁止公开与"个人或者家庭事务"有关的信息。国际上对隐私保护的重要法律文件是 1948 年的《联合国人权宣言》,明确地保护居所和通信的隐私不受侵犯。其第 12 条规定:"任何人对其隐私、家庭、房屋或者通信均不受武断干扰,其尊严或者名誉不受攻击。任何人均有权对这种干扰或者攻击获得法律保护。"信息技术发展到 20 世纪六七十年代,计算机系统所具有的庞大的监视能力推动了法律的进步,有利于规范个人信息的收集和处理。世界上第一个个人数据保护法源自德国黑森州(1970 年),接着,瑞典(1973 年)、

律规制的重点与其说是个人信息,不如说是"个人信息处理活动"更为贴切。[5]许多国家或地区的法律名称中为此专门突出了"处理"概念,如欧洲理事会、欧盟、圣马力诺、冰岛、希腊、丹麦和我国台湾地区。

对于名称问题,专家建议稿采用的是个人信息概念,而不是隐私或者个人数据概念。这种选择主要是基于以下几个考虑:

首先,数据这一概念在我国法律中比较生僻,它主要适用于技术领域,如数据库、数据交换。因此,如果法律名称采用它,对于普通公众会产生一定的理解困难,不利于法律的实施和普及。同样的道理,在我国,对于隐私概念的理解也比较狭窄,[6]主要是把它作为民事权利中的一种,当做名誉权的一部分。并且,即使这样狭窄的理解,也仍然主要停留在学术界,现行的民法通则并没有明确提到隐私权或规定隐私概念。因此,如果法律名称中采用它,一是因为其原意太狭窄,无法包容个人信息权利这样一种新型的公法权利种类,而且,也容易产生一词多义的问题,造成理解上的混乱。相比之下,个人信息概念,含义清晰,容易理解,使用它不会导致理解上的歧义或混乱(当然,在本文中,除非特别加以区分,三个概念是互换使用的)。

其次,在我国,随着信息化的推进,尤其是信息化法律体系的逐步形成,使诸如政府信息、个人信息、信息安全、信息资源等概念迅速普及。采用个人信息概念,不但与信息化和信息化法律体系建设的大背景符合,也可以与制定中的政府信息公开条例遥相呼应。

再次,由于欧盟与美国在个人信息保护问题上的不同认识,使个人数据概念与隐私概念在一定程度上被贴上了类别标签,成为各自阵营的标志。并且,可以预见,在未来的国际贸易和国际关系中,围绕这个问题,两大阵营的争议会进一步加剧。因此,既不选择标志欧盟的

美国(1974 年)、德国(1977 年)和法国(1978 年)相继制定了法律。在此过程中,产生了两个国际文件:1981 年欧洲理事会制定的关于保护自动处理的个人数据的公约和经合组织保护隐私与跨境个人数据流指南,对电子数据的处理规定了具体的规则。这些规则将个人信息描述为数据,并从收集、储存到传播的每个环节都给予保护。这两个协议对各国个人数据保护法的制定和实施产生了深远的影响。1995 年,欧盟制定了个人数据保护指令,以协调成员国对个人数据的法律保护水平,并保障数据在欧盟范围内的自由流动。欧盟指令要求成员国政府保证欧盟居民的个人信息被传送出或者在欧盟境外被处理时,必须得到同等水平的保护,拒绝提供同等保护的国家可能无法与欧盟进行信息交换。欧盟指令的这一要求给欧盟以外的国家造成了很大的压力,推动了世界范围内的制定个人信息保护法的高潮。

② 关于隐私,国际上通常认为,隐私权包括以下四个方面的内容:**信息隐私权**:涉及制定规则,以调整对诸如信用信息、医疗与政府档案等个人数据的收集和处理,它也称为"数据保护";**身体隐私权**:涉及保护个人的身体,对抗诸如基因测试、药品测试和非法搜查等侵犯性的程序;**通信隐私权**:涉及通信、电话、电子邮件和其他形式的通信的安全和隐私;**地域隐私权**:涉及对侵入家庭以及

个人数据概念,也不选择标志美国的隐私概念,体现的是一种独立的第三种声音。这样,不容易被别人贴标签,有利于我国在未来的国际贸易和国际交往中掌握主动,进退自如。

同时,考虑到汉语的使用习惯,专家建议稿在法律名称中并未使用"处理"概念,以保持法律名称的简洁性。但是,法律在总则部分对"处理"概念进行了专门的界定,强调了其作为核心概念的重要性。并且,在各章的具体规定中,也都体现了本法的调整对象是个人信息处理活动中的个人信息保护。

第二,关于欧盟与美国两种立法模式问题

法律是社会生活的集中反映。每一个国家的个人信息保护法反映的都是本国独特的社会生活,世界上没有任何两个国家的个人信息保护法会完全一样。从这个意义上看,不存在所谓的两种立法模式问题,或者换句话说,每个国家的法律都是自成一种立法模式。本报告之所以专门区别欧盟与美国两种立法模式,主要是就这两个实体在世界上的经济、政治地位以及它们对其他国家个人信息保护立法的影响力而言的。当然,这种区分也是国际上共同采用的一种分类方式。⑦

欧盟毫无疑问是个人信息保护立法的模范和先驱。欧盟国家最先关注信息通信技术对社会的影响问题,并导致欧盟于 1995 年制定了欧盟数据保护指令(1998 年 10 月开始生效)。欧盟指令价值倾向明显,覆盖范围广泛,规制程度深,执行机制健全。⑧在欧盟指令的要求下,所有欧盟国家(新近入盟十国除外)均已完成了新一轮的个人信息保护立法或者修法工作。尤其是,欧盟指令规定,第三

诸如工作场所或者公共场所等其他环境设立限制,包括搜查、电视监控以及核查证件等行为。应该说,这种解释是对隐私权概念最为广义的理解。一般语境下,尤其是在个人信息保护立法中,隐私权与个人信息保护概念可以互换使用。

③ 由于欧盟与美国在个人信息保护问题上已经形成了差异比较大的两种不同思路,实践中,"个人数据"与"隐私"的差别使用,就社会心理层面而言,可能会带有一定的价值判断或路径选择的意义。

④ 当然,个别国家,如阿根廷,个人信息保护法也适用于法人信息。这种情况非常罕见,没有普遍性。

⑤ 因为一旦禁止随意收集个人信息的目的达到,在个人信息的收集阶段就会遇到法律障碍,实际上不会进入形成特定个人信息的阶段。

⑥ 我国法律传统中"普天之下,莫非王土;率土之滨,莫非王臣"的国家观念,与西方的"风能进,雨能进,国王不能进"的权利观念,存在比较巨大的差别。现代版的陕西"家中看黄碟事件"应该说再一次凸显了这种差别。

⑦ 两者之间的根本分野,参见 Aaron Lukas, *Safe Harbor or Stormy Waters? Living with the EU Data Protection Directive*, Center for Trade Policy Studies, 2001, p. 16。

⑧ 按美国官方的正式评价,欧盟的这种立法模式是一种"一刀切"(one-size-fits-all)式的规制模式。

国的隐私法律只有经欧盟委员会判定达到“充分的”保护标准,才能自欧盟向其进行跨境个人信息传输。这样,非欧盟国家纷纷开始制定个人信息保护法,以满足欧盟指令的要求。虽然世界上制定个人信息保护法的国家很多,但迄今为止,只有加拿大、阿根廷、匈牙利和瑞士通过了欧盟的“充分性”判断标准。

美国是一个尤其重视企业的创造力与创新性的国家,其权利法案对传统个人权利的保护对世界各国宪法也产生了重大的历史影响。对于网络和现代通信技术所带来的海量的个人信息收集、存储和处理,根据美国官方的说法,它们既有利于跨境贸易和电子商务,也会引起对个人隐私权的担忧。美国政府的政策取向是,既要在国际范围内保护个人隐私,又不应阻断跨境信息流,影响电子商务和跨境贸易。美国政府希望通过对隐私保护采取平衡的规制方式,创造有利于创新的最佳增长环境。美国官方认为,美国的规制方式更加注重防止对个人信息滥用所造成的实际危害,因此可以保持商界最大的参与。相反,欧盟指令不加区分地适用于所有的行业,适用于个人数据处理的所有环节。

在立法思路上,目前,美国没有设定隐私保护最低要求的综合性联邦法律;相反,其对隐私保护采取了一种灵活的策略。美国政府认为,自律机制(包括企业的行为准则,民间“认证制度”以及替代争议解决机制)配合政府的执法保障,可以有效地实现隐私保护的目的。[9]为此,美国政府一直保持与商界和消费者团体的对话,鼓励更多地保护隐私,采用自律性的隐私保护政策。此外,在某些高度敏感的领域,美国政府认为适宜通过相应的立法,保护个人信息。美国国会通过的法律所保护的高度敏感个人信息包括儿童信息、医疗档案以及金融数据。并且,美国行政当局已经制定了行动计划,以进一步防止身份盗窃、发送垃圾邮件以及未经授权使用社会保险号等行为。为实

9 美国有学者研究得出结论,认为美国方式对消费者隐私的保护优于欧盟国家,可参见,Karim Jamal, Michael Maier and Shyam Sunder, Regulation and the Marketplace, *REGULATION*, 38 (winter 2003 ~ 2004)。

现这些目标,美国联邦贸易委员会已经宣布了一项重要的隐私保护执法计划,增加资源,保护消费者的消费信息不被滥用。

在国际上,美国政府一直通过各种国际组织,如经合组织、全球电子商务对话(Global Business Dialogue on Electronic Commerce)、泛大西洋商务对话(Trans-Atlantic Business Dialogue)以及各种消费者组织,推行其隐私保护灵活策略。经合组织1980年制定的隐私保护与跨境数据流指南,1998年《全球隐私网络渥太华宣言》,都明显地体现了美国的策略,强调了自律规制的重要性。目前,经合组织正在进行的项目包括进一步鼓励使用隐私保护技术,加强对使用者网络隐私意识与观念的培养。同时,在APEC,也在讨论、起草一份隐私保护框架,包括隐私保护的原则与实施机制。APEC隐私保护框架以经合组织指南为主要参考,争取在个人信息保护与信息的自由流动之间保持平衡,也反映了美国在隐私保护问题上的策略。该框架已经于2004年11月在APEC领导人峰会上最后通过。

尽管欧盟委员会从未对美国的个人数据保护体系发表过正式意见,但美国自律式的隐私保护体系能否通过欧盟的"充分性"保护标准在欧盟一直遭到许多怀疑。为此,美国对欧盟以及其成员国进行强力游说,希望让它们承认美国达到了充分保护的水平。1998年,美国开始与欧盟就隐私保护的"安全港"协议进行协商,以保证数据的跨界流动。在这种体制下,由美国公司自愿做出承诺,表明遵守由美国商务部和欧盟委员会内部市场司制定的一系列隐私原则,这样,这些公司就被假定达到了充分保护的要求,可以继续接受来自欧盟的个人数据。如果美国公司违反这些承诺,美国联邦贸易委员会与法院可以以虚假陈述为由对其加以惩处,但实践中基本上是由业界进行自我管制。美国与欧盟对"安全港"协议的谈判进行了近两年,期间受到隐私保护团体与消费者团体的猛烈批评。2000年7月初,欧盟议

会甚至通过一项决议,要求欧盟委员会重新与美国谈判,以提供个人信息的充分保护。不过,2000 年 7 月 26 日,欧盟委员会批准了协议。但是,欧盟委员会同时答应,如果对欧盟居民的救济被证明不充分,它将会重新开启谈判。

"安全港"协议要求所有签字的组织对其收集信息的种类、使用的目的以及可能披露给的第三方等,为个人提供"清晰和明显的"通知。这种通知必须在收集任何个人信息时或者实践可行之时提供。如果信息准备披露给第三方或者用于不相关的目的,个人必须能够明示选择拒绝被收集这种信息。如果是敏感信息,必须经过个人明确地明示同意这种收集。如果第三方参加"安全港"协议或者如果第三方签署保护数据的合同,签字的组织可以向该第三方传送数据。参加的组织必须保证个人可以获知有关他们个人的任何信息,并有机会改正、修改或者删除不准确的信息。截至 2003 年 12 月 2 日,共有 420 个美国组织签署加入了"安全港"协议。

2002 年 2 月,欧盟委员会发布了欧美"安全港"协议实践运作情况的第一份报告,认为协议的主要内容已经到位,如果个人觉得其权利受到侵犯,存在提起申诉的结构。不过,委员会也发现签署了"安全港"协议的组织缺乏足够的透明度,并且,并非所有的争议解决提供者都遵守协议的隐私保护原则。在"9·11 事件"的影响下,2004 年 5 月 17 日,欧盟与美国签署《航空安全条约》,向美国提供始自欧洲的航班上的乘客的 34 项信息,此举受到隐私保护团体更加强烈的批评。

我们认为,不论是欧盟立法模式还是美国立法模式,都有其合理的地方,更重要的是,都有各自的价值观和社会基础作为支撑。作为第三方,比较好的选择是分别汲取其有益的经验,并结合本国的国情做出具体的制度设计。日本学者在这个问题上观点非常鲜明,值得我们借鉴。在与我们的交流过程中,日本学者丝毫不讳言日本的个人信息保

护立法外形上类似欧盟立法模式,实质上采纳了许多美国的做法。专家建议稿应该说也充分吸收、借鉴了欧盟与美国的经验,在每个具体的制度设计上都充分考虑了将两者的长处结合到一起,并反映中国社会生活的现实与长远需要。[10]

[10] 由于在可以预见的将来,欧盟判断非欧盟国家法律充分性的标准仍会保持其"高门槛",因此,专家建议稿在起草过程中并没有以通过欧盟的标准为立法目标,而是以解决中国的现实问题为主要考虑。如果中国与欧盟未来就中国个人信息保护立法的保护充分性问题展开谈判,中国应该以自己个人信息保护的整个法律体系,而不仅仅是一部个人信息保护法,展示个人信息保护制度的充分性。

第三,制定个人信息保护法的意义与必要性

随着我国社会的不断发展,无论是各政府部门及被授权或者受委托行使一定行政职能的组织,还是各种非政府部门,在进行活动时,往往都会收集、保存大量的个人信息。特别是随着信息技术的不断发展,批量处理和传递个人信息已经越来越容易。个人信息遭到不当收集、恶意使用、篡改以至扰乱公民个人安宁生活进而危及其生命、财产安全的隐患也就会随着出现。[11]另外,如果人们普遍对个人信息没有安全感,必然会本能地拒绝任何信息处理或者提供虚假的信息,由此制约信息的自由流动,加大市场主体的交易成本。因此,对于我国而言,通过立法尽快建立个人信息保护制度已是刻不容缓,具有重要的现实意义。

[11] 中央电视台2004年10月16日播出的《今日说法》节目报道,一家企业在一次大型招聘会上不慎遗失了一位女求职者的求职登记表格,表格上面记载有该求职者的基本个人信息。一个犯罪分子拾得该登记表格,冒充该企业的招聘人员,对求职者实施了犯罪,并杀害了求职者

1. 确立个人信息保护制度是保护个人权利的需要

现在,人们已充分体会到信息化为生活和工作带来的种种便利,而与此同时,个人的合法权益也因此面临着被侵害的可能。通过各种可以识别出个人或者同相关信息结合而可识别出个人的信息,便可以勾画出一个人的全貌或者把握其某一方面的特征。现实中,有关政府部门超出职权范围、有关非政府部门超出其业务目的收集利用个人信息的现象随处可见。比如,我们可以发现,许多学校以防范考试作弊、加强校内管理为名,安装闭路电视监控设

备,以至于学生的一举一动尽在其监控之内。[12]一些地方在制作各种形式的社保卡或其他电子卡时,收集的个人信息有的多达一百多项,存在严重的滥用危险。而且,由于对个人信息的保存、转让缺乏有效的规范,个人信息被随意篡改、滥用以及被非法转卖牟利的现象时有发生。比如,房地产开发商或其职员非法转卖购房者相关个人信息的现象已是十分常见,而近来又发现了专门出卖他人电子邮箱地址的行为。[13]又比如,一些地方在信息化的名义下,一窝蜂地研发各种信息检索系统,将个人信息不加区分地纳入其中,但是,对于可收集的个人信息的范围、可进行相关检索的主体、检索主体可检索信息的范围等均缺乏明确的规定,这对于个人的信息安全和生命财产安全必将形成极其严重的威胁。[14]另外,个人对于有关组织所收集、保存的本人信息无权查阅,以至于对于自己的哪些信息为他人所掌握、该信息是否与事实相符等往往无从把握,现实中有关组织基于有误的个人信息而对本人做出各种决定的现象并不鲜见。当人们体味着信息化给生活带来的种种便利的同时,又不得不面对个人生活空间逐步缩小的现实。因此,随着信息化社会中大量个人信息被收集利用,必须尽快确立我国的个人信息保护制度。同时,个人信息保护法对于控制信息时代行政权在高技术领域的滥用,实现依法行政,保障基本人权,也有重要意义。[15]

2. 确立个人信息保护制度是有效利用信息资源的需要

个人信息的不当处理不但会侵害个人的合法权益,还会因失去人们的信任而导致所处理信息的失实,使信息及信息处理丧失本应具有的价值。交流与共享是信息的价值所在,而事实上,随着我国信息化的发展,促进信息流动和交流的最大化已经成为社会发展的迫切需求。比如,公安系统于2001年实现了11.3亿人口数据的计算机管理,

⑫ 据媒体报道,上海某学校在学校内部安装了大量摄像头,不分时间和对象进行监控,并通过校内闭路电视公布其认为违反校规的学生录像,一对男女学生就因在教室内做出亲昵动作而被当众公开,被周围同学讥讽,遭受了严重的心理压力,而最终将母校告上法庭(中央电视台新闻频道2004年2月15日播出的"面对面"栏目对该案进行了报道,题为《魏罡:成长的烦恼》,其文字材料请参见"央视国际"网站,地址为 http://www.cctv.com/news/society/20040216/1003891.shtml)。

⑬ 《作家文摘》2004年1月16日第7版

⑭ 比如,湖南省就开通了身份证核查系统,人们可以通过拨打电话、上网或者手机短信的方式查询湖南户籍居民的基本身份信息。参见《北京青年报》2003年11月10日第A1版。据报道,南京市将启用婚姻登记信息系统,以后所有南京人的婚姻状况都将上网,市民的婚姻状况可以通过民政网查询。婚姻当事人的身份证号码、住址,以及什么时候、在什么地方、是否曾登记结婚,一查便知,开单身证明、制止重婚等将变得非常有效。对此,法学专家产生了不同的意见,有人认为这种做法是应该的,不应该以保护隐私为名来否定南京市的做法;有专家则认为南京市将启用的婚姻登记信息系统的使用者不是相关人员,而且公布的信息过多,已构成了对隐私权的侵犯。参见教

仅2001年,其全国人口信息管理系统就为全国公安机关提供查询服务780万人次,为政府部门提供查询服务472万人次,为群众提供查询服务460万人次,协助破案20.4万起,挽回经济损失七亿多元。2003年9月2日正式全面启动的"金盾工程"从2004年上半年开始逐步向全国公安系统提供信息服务,2005年底基本实现全国联网查询和综合开发利用,期间逐步满足其他政法部门、有关部委和社会用户对公安信息资源的共享需求,到2007年基本实现公安工作信息化。[16]但是,信息的利用和共享绝不能以牺牲个人的合法权益为代价,否则,便会失去其存在的合法性,最终将会因信息失实而丧失存在的必要性。另外,如何共享、共享哪些信息等问题如果不明确的话,也会制约共享,阻碍对信息资源的有效利用。以我国银行业实行的储蓄实名制为例,《个人存款账户实名制规定》规定,除法律法规另有规定以外,金融机构不得向任何单位或者个人提供有关个人存款账户的情况,并有权拒绝任何单位或者个人查询、冻结、扣划个人在金融机构的款项。不久前就发生过某人因输错账号而通过ATM机将钱款汇入他人账户的案件。汇款人要求银行提供被错汇入钱款的账户户主的信息以便追回错汇的钱款,但遭到银行拒绝。[17]银行的做法完全符合现行法规的规定,问题恰恰在于现行法规仅考虑到了保密,而缺乏共享方面的合理规定。在国外,有着完善的个人信息保护体系,并且,一般均会允许为保护第三人的合法权益而依照一定程序向其提供个人信息。[18]因此,如果没有个人信息收集利用方面的完善制度,不但个人的合法权益会受损,更会阻碍我国信息化的进程。

3. 确立个人信息保护制度可以促进我国的电子商务和电子政务健康发展

随着信息化的不断发展,电子商务这一被称为21世

祥菲:"婚姻资料上网是否侵犯隐私权",载《人民法院报》2004年8月3日第B2版。

⑮ 据报道,上海准备在2010年之前安装20万个监控摄像头,建立全面的"社会防控体系"。这一消息在市民中引起了广泛的关注,引起此举是否会侵犯隐私权的许多议论。另外,公安部门力争的"手机卡销售实名登记"制度,也引起广大用户的争议。支持者认为可以加强对手机短信的控制和打击犯罪,反对者认为会侵犯个人隐私,提升交易成本。

⑯ 《法制日报》2003年9月3日第1版。

⑰ 中央电视台《今日说法》栏目2004年1月29日报道了该案件,题为"转错账之后",其文字资料刊载于"央视国际"网站,地址为www.cctv.com/news/society/20040129/100424.shtml。

⑱ 比如许多国家的个人信息保护法均规定,为保护他人生命、身体或者财产而又很难取得个人信息的本人的同意的,可以不经其同意向他人提供有关个人信息。这实际上可以避免一味保护个人信息而使他人的合法权益受损。

纪经济增长原动力的商业模式在国民经济中的作用越来越重要,电子政务也已被视作建设高效、透明政府的重要举措。在网上交易过程中,消费者的许多个人信息往往会在知情或者不知情的情况下被商家收集,[19]消费者有时就会因担心个人信息的安全而放弃进行网上交易,仍旧选择传统交易方式,这在很大程度上制约着我国电子商务的发展。同样,没有安全且值得信赖的个人信息保护体系,也就不可能建成值得人们信赖的电子政府,我国的电子政务建设必将受到影响。可以说,个人信息保护制度,是推进电子商务与电子政务的一项基础性工程。

⑲ 比如,电脑接入互联网后,电脑中的cookie程序可以记录已登陆网站的信息,以缩短下一次登陆同一网站时打开网页的时间。通过这一程序,网站也可以收集到上网用户包括个人偏好等在内的许多个人信息。对此,可以通过禁用cookie予以避免。但是,木马程序等许多恶意程序、电脑病毒在窃取上网用户个人信息方面的危害则是防不胜防。

4. 制定个人信息保护法可以促进国际交往,在国际关系中保持主动

在国际舞台上,个人信息保护不仅是一个基本人权问题,也极有可能成为某种新的贸易壁垒。实际上,这种趋势已经非常明显并且会进一步加剧。在人权层面上,一旦我国批准《公民与政治权利公约》,对个人信息保护的国际压力会越来越大。在国际贸易层面上,随着新加入欧盟的国家逐步达到欧盟指令的要求,欧盟以及其他国家完全有可能根据对第三国个人信息保护水平的判断,对个人信息的跨国流动做出单方面的限制,进而影响到整个国际贸易的正常进行。尽管美国在个人信息保护问题上与欧盟有不同的看法,并且,美国正尽量利用其影响力在诸如经合组织、APEC等框架内推行其理念,但是,最终效果现在尚难预料。无论如何,一个个人信息保护法制不健全的国家肯定会在国际人权与国际贸易两方面腹背受敌,受到其他国家或国际组织的打压。与其届时被动改变,不如现在主动改革,通过制定个人信息保护法,树立良好的国际形象,在国际关系中保持主动。

5. 确立个人信息保护制度可以进一步推动政府信息公开工作

经过多年的实践和理论研究,我国在推进政府信息公开方面不断取得进步,相关的制度构建工作正在顺利推进,“公开为原则,不公开为例外”的观念已经深入人心。可以说,实现政府信息的共享,有效利用信息资源,是推进我国政府信息公开的一大动力。政府信息公开中很重要的一点是要明确不公开信息的范围,这其中就包括对个人信息的保护问题。如果没有完善的个人信息保护法,对何谓个人信息、如何保护个人信息、如何在个人信息的公开与不公开之间做出选择等做出明确且具有可操作性的规定,有关部门就有可能以保护个人信息之名,拒绝公开政府信息,或者以公开政府信息之名,公开他人个人信息。由此可见,完善的个人信息保护制度同政府信息公开制度有着相辅相成、不可分割的关系,没有完善的个人信息保护制度,绝不可能有真正的政府信息公开制度。

6. 制定个人信息保护法可以推动我国信息化法律体系的建设

大力推进国民经济和社会信息化,以信息化带动工业化,实现跨越式发展,是党中央、国务院的一项战略决策。全面推进信息化,立法工作是其中的一个重要环节,是一项基础性的工作。只有尽快构建有中国特色的信息化法律体系,才能为信息化建设提供制度保障,推动信息化的进程。《国家信息化领导小组关于我国电子政务建设指导意见》明确地提出要“加快推进电子政务法制建设,加快研究和制定电子签章、政府信息公开及网络与信息安全、电子政务项目管理等方面的行政法规和规章”。《国家信

息化领导小组2004年工作要点》再一次将信息化法律法规建设放在了重要的地位,提出"继续推动《电子签章法》、《政府信息公开条例》的制定,研究起草《个人数据保护法》、《网络信息安全条例》","加强信息化立法调研工作,研究提出信息化发展的相关立法计划"。尽管我国信息化法律体系如何构建还需要进一步的研究和探索,但个人信息保护法毫无疑问是其中的一部基础性法律,是构建个人、企业与政府三方良性互动关系中最为重要的环节之一。制定个人信息保护法,必将推动我国整个信息化法律体系的建设。

第四,我国个人信息保护法律的现状

由于各个方面的原因,我国个人信息保护法律的现状不容乐观。总体状况是法律规定比较零散、无体系,保护范围狭窄,并且缺乏统一的执行机制与机构。

1. 宪法对个人隐私权利的保护

《中华人民共和国宪法》第38条规定:"中华人民共和国公民的人格尊严不受侵犯。禁止用任何方法对公民进行侮辱、诽谤和诬告陷害。"本条的规定可以说是个人信息权利的直接来源,它虽然没有明确出现"隐私保护"的字眼,但是在实质意义上,通过对上述权利的保护,公民个人的隐私也间接不受侵犯。同理,宪法第39条和第40条也可以当做我国个人信息权利的直接宪法依据。另外,诸如宪法第41条、第47条、第51条和宪法修正案第24条,则可以作为宪法对个人信息权利的间接保护依据。

2. 部门法中的规定

我国的法律法规中没有出现“隐私权”的字眼,没有任何一部法律冠有“隐私”之名,当然更没有法律法规冠以“个人信息保护”之名。我国隐私保护的法律大体涉及以下三个方面:

(1)人格、名誉方面的隐私

《中华人民共和国民法通则》第 101 条规定:“公民、法人享有名誉权,公民的人格尊严受法律保护,禁止用侮辱、诽谤等方式损害公民、法人的名誉。”第 102 条规定:“公民、法人享有荣誉权,禁止非法剥夺公民、法人的荣誉称号。”这两条规定是宪法第 38 条在民法领域的具体体现。随后颁布的最高人民法院《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)》对此做了进一步说明:“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。”另外,最高人民法院审判委员会第五百七十九次会议还专门就法院如何审理名誉权案件通过了最高人民法院《关于审理名誉权案件若干问题的解答》,对全国各级法院在审理此类案件中遇到的一些典型问题,如侵犯名誉权的主体,因侵犯名誉权而招致的赔偿的数额和范围等都做了解答。此外,对于那些侵犯名誉权较为严重的行为,刑法第 246 条第 1 款规定:“以暴力或者其他方法公然侮辱他人或者捏造事实诽谤他人,情节严重的,处三年以下有期徒刑、拘役、管制或者剥夺政治权利。”同时,鉴于妇女儿童的相对弱势地位,《中华人民共和国妇女权益保护法》(1992 年)第 39 条规定:“妇女的名誉权和人格尊严受法律保护。禁止用侮辱、诽谤、宣扬隐私等方式损害妇女的名誉和人格。”《中华人民共和国未成年人保护法》规

定,全社会都应当尊重未成年人的人格尊严,不得进行侮辱其人格的行为。

(2)个人信息方面的隐私

个人信息,是指涉及个人的已被识别的或可被识别的任何资料,它与国外所说的个人数据的范围大致相同,国内法律在几个大的涉及个人信息的领域都做了保护性规定。

①邮件和电子信件隐私

《中华人民共和国刑法》第252条规定:"隐匿、毁弃或者非法开拆他人信件,侵犯公民通信自由权利,情节严重的,处一年以下有期徒刑或者拘役。"《中华人民共和国邮政法》第4条规定:"通信自由和通信秘密受法律保护。除因国家安全或者追查刑事犯罪的需要,由公安机关、国家安全机关或者检察机关依照法律规定的程序对通信进行检查外,任何组织或者个人不得以任何理由侵犯他人的通信自由和通信秘密。"而且在随后由国务院颁布的《中华人民共和国邮政法实施细则》对这一条还做了进一步的程序性规定:"因国家安全或者追查刑事犯罪需要,公安机关、国家安全机关、检察机关检查、扣留邮件,冻结汇款、储蓄存款时,必须依法向相关县或者县级以上的邮政企业、邮电管理局出具相应的检查、扣留、冻结通知书,并开列邮件、汇款、储蓄存款的具体节目,办理检查、扣留、冻结手续后,由邮政企业指派专人负责拣出,逐件登记后办理交接手续;对于不需要继续检查、扣留、冻结或者查明与案件无关的邮件、汇款、储蓄存款,应当及时退还邮政企业。邮件、汇款、储蓄存款在检查、扣留、冻结期间造成丢失、损毁的,由相关的公安机关、国家安全机关、检察机关负责赔偿。"邮政法第6条第2款规定:"除法律另有规定外,邮政企业和邮政工作人员不得向任何组织或者个人提供用户使用邮政业务的情况。"但其第21条却规定,邮政工作人员可以在现场检查信件以外的其他邮件,用户交寄的信件

必须符合准寄内容的规定,必要时邮政企业及其分支机构有权要求用户取出进行验视。《中华人民共和国邮政法实施细则》对禁寄的物品做了详细的规定。在该法之后,各个省、自治区和一些较大的市都结合本地区的实际情况制定了邮政条例或邮政管理办法。

随着电脑在中国的普及,电子邮件逐渐取代传统的书信而成为人们之间交往的一种重要方式,不仅是私人信件,包括企业间的业务往来、政府指令的传达都基本实现了网上操作。1997 年,经国务院批准,公安部颁布了《计算机信息网络国际联网安全保护管理办法》,其第 7 条规定:"用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定,利用国际联网侵犯用户的通信自由和通信秘密。"但同时也规定了用户必须进行登记和接受安全检查的义务。《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》第 18 条规定:"用户应当服从接入单位的管理,遵守用户守则;不得擅自进入未经许可的计算机系统,篡改他人信息;不得在网络上散发恶意信息,冒用他人名义发出信息,侵犯他人隐私;不得制造、传播计算机病毒及从事其他侵犯网络和他人合法权益的活动。"但在后面的第 19 条中又规定:"国际出入口信道提供单位、互联单位和接入单位应当保存与其服务相关的所有信息资料;在国务院信息化工作领导小组办公室和有关主管部门进行检查时,应当及时提供有关信息资料。"

1999 年,中国设立了国家信息安全测评认证中心,它负责保护互联网上的国家机密和商业秘密,辨认网络用户身份,明确权利和责任,目的在于保护个人和政府使用网络,通过对非授权使用信息的监控达到保护信息的效果。2000 年,全国人大常委会通过了《全国人民代表大会常务委员会关于维护互联网安全的决定》,对利用计算机网络侵犯个人隐私的行为也做了专门规定。同年,国务院颁布了《互联网信息服务管理办法》,第 14 条规定:"从事新

闻、出版以及电子公告等服务项目的互联网信息服务提供者,应当记录提供的信息内容及其发布时间、互联网地址或者域名;互联网接入服务提供者应当记录上网用户的上网时间、用户账号、互联网地址或者域名、主叫电话号码等信息。"2002 年,国务院又通过了《互联网上网服务营业场所管理条例》,要求"互联网上网服务营业场所经营单位应当对上网消费者的身份证等有效证件进行核对、登记,并记录有关上网信息。登记内容和记录备份保存时间不得少于六十日,并在文化行政部门、公安机关依法查询时予以提供。登记内容和记录备份在保存期内不得修改或者删除"。

②健康医疗信息隐私

由于病人的医疗信息往往关系到患者的名誉和内心感受,因此对病人的病历档案应当加以特别的保护。1988 年由卫生部颁布的《医务人员医德规范及实施办法》中就要求医务人员要"为病人保守医密,实行保护性医疗,不泄露病人隐私与秘密"。1999 年 5 月 1 日开始施行的《中华人民共和国执业医师法》规定医生不得披露治疗中获得的健康信息,违反的需要追究刑事责任。尽管如此,病人信息被泄露的情况仍时有发生。为此,卫生部和国家中医药管理局于 2002 年制定了《医疗机构病历管理规定》,其中对病历的管理、使用都做了详细的规定。除涉及对患者实施医疗活动的医务人员及医疗服务质量监控人员外,其他任何机构和个人不得擅自查阅该患者的病历。同年 4 月 4 日颁布的《医疗事故处理条例》中也有类似的规定,并进一步强调医疗机构在复制或者复印病历资料时应当有患者在场。2004 年修订的《中华人民共和国传染病防治法》明确规定了传染病人的个人隐私受到法律的保护,并规定了违反规定者需要承担刑事责任。

艾滋病病人是一类特殊人群,他们不但承受着病痛的困扰,还要时时刻刻担心受到别人的歧视,因此对于他们

的个人信息法律也做了特别的保护。1999 年 5 月,卫生部经国务院批准,发布了《关于对艾滋病病毒感染者和艾滋病病人的管理意见》,其中规定:"从事艾滋病病毒感染者和艾滋病病人诊断、治疗及管理工作的人员,不得向无关人员泄露有关信息。任何单位和个人不得将艾滋病病毒感染者和艾滋病病人的姓名、住址等个人情况公布或传播,防止社会歧视。"在此前后,许多的省市都颁布了有关艾滋病防治的管理办法,如上海市 1999 年 3 月 1 日开始施行的《上海市艾滋病防治办法》中规定:"任何单位和个人应当为艾滋病病人和艾滋病病毒感染者保密,不得泄露艾滋病病人和艾滋病病毒感染者的姓名、住址、工作单位和病史等资料。"

③储户存款信息隐私

公民在银行办理信用卡或购房贷款时经常会填写一些属个人隐私范围的信息,如身份证号码、家庭住址、私人电话号码,必要时还须向有关机构提供自己的银行存款数额等。这些信息一旦泄露,将给储户带来不小的麻烦。针对此种情况,《中华人民共和国商业银行法》第 6 条规定:"商业银行应当保障存款人的合法权益不受任何单位和个人的侵犯。"第29 条规定:"商业银行办理个人储蓄存款业务,应当遵循存款自愿、取款自由、存款有息、为存款人保密的原则。对个人储蓄存款,商业银行有权拒绝任何单位或者个人查询、冻结、扣划,但法律另有规定的除外。"《个人存款账户实名制规定》规定,除法律法规另有规定以外,金融机构不得向任何单位或者个人提供有关个人存款账户的情况,并有权拒绝任何单位或者个人查询、冻结、扣划个人在金融机构的款项。另外,银行的内部守则也对保护客户的隐私做了完善的规定,如《中国工商银行员工行为守则》中要求员工必须"严守客户秘密。对于客户提供的信息资料,员工有保密的义务,以维护客户的合法权益。除依法可以提供或客户同意提供的信息外,员工无权擅自

披露客户信息”。在2003年修订过的中国人民银行法中要求“中国人民银行的行长、副行长及其他工作人员,应当依法保守国家秘密,并有责任为与履行其职责有关的金融机构及当事人保守秘密”。

非常值得一提的是,2003年12月22日上海市率先在全国通过了个人征信方面的地方性法规——《上海市个人信用征信管理试行办法》。该法分为8章33条,对个人信用信息的采集、加工、处理、提供等都做了详细的规定。在征信原则一条中,它将“尊重个人隐私”明确地作为征信的原则之一,为征信活动的进行定下了一个基调,即不得以征信为目的而滥用公民的个人信息。同时,它还规定了采集个人信用信息中使用的方法,可以采集的信息和禁止采集的信息(如涉及个人的敏感数据),尤其是对征信机构在对外提供所掌握的信息条件设定了严格的限制,并且允许被征信个人对已收集的涉及自己的信息提出异议,要求征信机构在法定期限内作出处理。这些规定,较之以前分散在各个法律文件中的保护隐私的规定更为系统、完备。据悉,中国人民银行牵头起草的“征信管理条例”中也将涉及对个人隐私在法律条文上的界定。届时,储户的信息保护将走上更加正规的道路。

④未成年人的信息隐私

未成年人是一个特殊群体,他们由于没有或是没有完全的法律上的行为能力,因此其大量的民事行为都是由其监护人来完成的。这就产生了如何保护这一特定人群的信息隐私的问题。《中华人民共和国未成年人保护法》第30条规定:“任何组织和个人不得披露未成年的个人隐私。”第31条规定:“对未成年人的信件,任何组织和个人不得隐匿、毁弃;除因追查犯罪的需要由公安机关或者人民检察院依照法律规定的程序进行检查,或者对无行为能力的未成年人的信件由其父母或者其监护人代为开拆外,任何组织或者个人不得开拆。”在新近修正的《北京市未

成年人保护条例》第49条规定:“任何组织和个人不得披露未成年人的个人隐私。对未成年人的信件,任何组织和个人不得隐匿、毁弃;除因工作需要由司法机关依照法定程序进行检查,或者对无民事行为能力未成年人的信件由其父母或者其他监护人代为开拆外,任何组织或者个人不得开拆。任何组织和个人未经未成年人的监护人同意,不得在互联网上收集、使用、公布未成年人的个人信息。”另外,对于未成年犯罪嫌疑人的隐私保护,法律也有相关规定。《人民检察院办理未成年人刑事案件的规定》中规定:人民检察院办理未成年人刑事案件,应当注意保护涉案未成年人的名誉。不得公开或者传播该未成年人的姓名、住所、照片及可能推断出该未成年人的资料。最高人民法院《关于审理未成年人刑事案件的若干规定》中也规定:“对在开庭审理时不满十六周岁的未成年人刑事案件,一律不公开审理。对在开庭审理时不满十八周岁的未成年人刑事案件,一般也不公开审理。如果有必要公开审理的,必须经过本院院长批准,并且应限制旁听人数和范围。”同时,对未成年人作证人的情形也做了特殊规定,即其可以不出庭。

(3)其他的重要个人隐私

①《中华人民共和国居民身份证法》

一直以来,居民身份证不仅承担着证实公民身份的角色,更是政府部门控制人口流动、维护社会秩序的有力手段。警察可以随时随地的要求某人出示身份证,而无须履行任何程序上的义务。为了保护公民的个人隐私不再被肆意侵扰,2003年6月28日,中华人民共和国人民代表大会常务委员会第三次会议通过了《中华人民共和国居民身份证法》,并于2004年1月1日起施行。该法第6条中规定:“公安机关及其人民警察对因制作、发放、查验、扣押居民身份证而知悉的公民的个人信息,应当予以保密。”第15条对警察可以检查居民身份证的情况做了详细规定,

但同时也规定在检查之前必须先出示证件。另外,第19条还规定,警察"泄露因制作、发放、查验、扣押居民身份证而知悉的公民个人信息,侵害公民合法权益的"必须承担相应的法律责任。这些规定使得身份证在本质上不再是政府机关监管公民的工具,而只是证明公民身份的凭证而已。

②婚姻、家庭方面的隐私

在过去的计划经济体制下,婚姻带有浓厚的行政色彩。不仅结婚要单位出示证明,去医院进行婚检,连生育也必须办理生育指标。在新修改过的婚姻法和《婚姻登记条例》中,免去了单位的证明义务和婚检的义务。另外,1994年的《中华人民共和国母婴保健法》中规定:"从事母婴保健工作的人员应当严格遵守职业道德,为当事人保守秘密。"

③服刑犯人的隐私保护

随着中国加入一系列的国际人权公约,对犯人的人权保护也提上了日程。《中华人民共和国监狱法》第7条第1款规定:"罪犯的人格不受侮辱,其人身安全、合法财产和辩护、申诉、控告、检举以及其他未被依法剥夺或者限制的权利不受侵犯。"但第18条又规定:"罪犯收监,应当严格检查其人身和所携带的物品。非生活必需品,由监狱代为保管或者征得罪犯同意退回其家属,违禁品予以没收。女犯由女性人民警察检查。"第47条规定:"罪犯在服刑期间可以与他人通信,但是来往信件应当经过监狱检查。监狱发现有碍罪犯改造内容的信件,可以扣留。罪犯写给监狱的上级机关和司法机关的信件,不受检查。"

④有关档案、统计方面的隐私保护

公民的个人档案记录了公民一生中最重大的个人信息,因此对于每个公民来说都希望有一套严密的法律体系来保护自己的档案不被非法利用。《中华人民共和国档案法》部分地满足了公民的愿望,对档案机构的设置及其职

责以及档案的管理都做了规定,但遗憾的是,整个法律对个人档案的保护着墨不多,而且由于缺乏个人查询自己档案的机制,使得很多人从出生到死亡都不曾见过自己的档案,这不可避免地会造成某些错误得不到纠正的情况。另外,统计也是一项非常容易触犯个人隐私的活动,《中华人民共和国统计法》中规定:"属于私人、家庭的单项调查资料,非经本人同意,不得泄露。""统计机构、统计人员违反本法规定,泄露私人、家庭的单项调查资料或者统计调查对象的商业秘密,造成损害的,依法承担民事责任,并对负有直接责任的主管人员和其他直接责任人员依法给予行政处分。"

第五,关于权利的性质与立法的依据

在国际社会,人们谈论个人信息保护问题时往往将其同隐私权保护相等同,而对隐私权的保障确实是个人信息保护的主要目的和逻辑前提。在最初的阶段,隐私权一直被作为普通私法中侵权行为法上的权利,意味着与个人私生活有关的信息不受公开以及属于私事的领域不受干涉的自由,是一种要求他人放任自己独处而不受打扰的权利。

人类社会进入20世纪60年代之后,随着计算机技术的不断发展,信息的大量收集、储存和利用成为可能,这使得隐私权受到侵害的可能性越来越大。因此,传统意义上具有消极、被动等特点的隐私权概念已显得过于狭隘,很难适应社会发展的需要。在这种情况下,出现了所谓"个人信息控制权"的理论,即"所谓隐私权,乃是指个人自由地决定在何时、用何种方式、以何种程度向他人传递与自己有关的信息的权利主张"。[20]这样,现代意义的隐私权在

[20] [日]奥平康弘:《知情权》,株式会社岩波书店1981年版,第384~385页。

具有消极、静态、阻碍他人获取与个人有关的信息等特性的同时,更具有了支配权的特点,具体表现为权利主体对与自己有关的信息进行收集、储存、传播、修改等所享有的决定权,按自身意志从事某种与公共利益无关的活动而不受非法干涉的个人活动自由权,其私有领域不受侵犯的权利,以及权利主体依法按自己意志利用与自己有关的信息从事各种活动以满足自身需要的权利。

按照对现代隐私权概念的理解,作为"个人信息控制权"的隐私权所保障的已不限于传统意义上的尚不为人所知、不愿或者不便为人所知的个人私事(即一般而言的隐私),而是扩展到了所谓的个人信息,即识别出或者可以识别出个人的所有信息,这些信息可以以文字、图表、图像等任何形式存在,并可以附载于纸张、电磁媒体等任何媒介之上。这种认识转变促使隐私权逐步由一种私法上的民事权利演变为一种公民在宪法上的基本人权。

隐私权的概念和理论最早产生于美国,由路易期·布兰代斯(Louis Brandeis)和萨莫尔·华伦(Samuel Warren)于1890年在《哈佛法律评论》上首次提出。正是在美国,隐私权被作为一项最为重要的宪法权利而不是普通的民事权利,以宪法惯例的形式得到学术与实务部门(包括联邦最高法院裁决)的确认。类似的,在法国,1958年宪法虽未明确规定隐私权,但法国宪法委员会通过1994年的一项裁决,确认宪法隐含了隐私权。在印度,1950年宪法没有明确承认隐私权,但早在1964年,印度最高法院就首次依宪法第21条做出裁决,认定宪法已隐含隐私权。在爱尔兰,宪法未明确提及隐私权,但爱尔兰最高法院裁决,公民有权援引宪法第40.3.1个人权利条款证明隐私权的存在。

隐私权这种基本人权地位在一系列的国际法律文件中同样得到了体现。1948年的《联合国人权宣言》,明确地保护居所和通讯的隐私不受侵犯。第12条规定:"任何

人对其隐私、家庭、房屋或者通信均不受武断干扰,对其尊严或者名誉不受攻击。任何人均有权对这种干扰或者攻击获得法律保护”。众多的国际人权文件均将隐私权视为一项重要的权利,《公民与政治权利公约》第17条,《联合国移居工人公约》第14条,《联合国儿童保护公约》第16条都采用了相同的表述。特别需要提到的是《欧洲人权公约》,该公约第8条规定:“(1)每个人都有权使其私人生活和家庭生活、其房屋和通信受到尊重。(2)除非根据法律规定,并且,为了国家安全、公共安全或者国家的经济福利,为了防止无序或者犯罪,为了保护健康或者为了保护其他人的权利与自由所必须,公共权力机关不得干预这种权利的行使。”该公约的执行机关是欧洲人权委员会与欧洲人权法院,它们在保护隐私权方面非常积极,一贯对第8条的保护进行扩张解释,对限制条件从严解释。实践中,如果政府对私人行为应该加以禁止而不予禁止,它们就会扩充第8条的保护范围,从政府行为扩张到私人行为。由于欧洲人权公约在许多欧洲国家具有直接的法律效力,因此,公约第8条的规定在这些国家实际上具有宪法地位,可以被法院援引裁决案件。

在许多国家的宪法中,隐私权的这种基本人权地位也得到了宪法的明确规定和保护。例如,阿根廷宪法第18条、第19条规定:“住宅、私人通信、私人文件神圣不可侵犯;对之搜查或征用的,由法律规定之。”第43条规定:“个人资料为公共机关、私人机构或专为提供信息服务之数据库留存的,有权获得涉及其个人的资料,知晓其个人资料使用的目的;资料错误或有歧视的,有权阻止对之使用,或予以校正、保密或更新。但新闻消息源的隐私不受影响。”巴西宪法规定了独特的人身资料权,以保证下述权利的实现:(1)申请人对于保存在政府机关或公共机构代理人处涉及本人的档案或资料的知情权;(2)申请人可以不通过司法或行政的秘密程序修正其个人信息的权利。保加利

亚宪法第41条规定:"(1)公民有寻求、获得和散布信息的权利,但行使此类权利时不得损害他人权利和名誉,不得损害国家安全、公共秩序、公共健康和公共道德。(2)公民有从国家机关和团体获得与其合法利益相关事情的信息,但以该信息未被法律规定为国家或其他的机密,以及不影响他人权利为限。"爱沙尼亚1992年宪法第42条规定:"中央或地方国家机关不得收集、储存意在规劝公民违背自由意愿的信息。"第44条第3款规定:"公民有权依法律规定程序,知晓中央及地方政府掌握或其档案中保存的个人信息,但为保护他人权利和自由、保护儿童血统秘密、预防犯罪、查证犯罪、澄清法庭事实时需要受到限制的例外。"希腊宪法2001年修正案在第9条增加一款,规定个人有直接保护其个人信息的权利。第9A条规定:"公民有权依法保护其个人信息不被收集、处理和使用,也有权不允许通过电子方式收集、处理、使用其个人信息。个人信息保护由独立机关实施。该机关的设立和运行由法律规定之。"秘鲁1993年宪法规定了全面的隐私、数据保护和信息自由权利。其宪法第2条规定,"公民享有如下权利:有权请求他所需要的信息而不必公开原因,有权通过支付合理的费用在法律规定的期限内从任何公共机构得到那一信息。涉及个人秘密的信息和法律规定的或者因为国家安全的原因而被明确排除的信息不必公开。"

在专家建议稿中,根据国际社会的普遍经验和本法规定的内容兼及政府机关与其他个人信息处理者的实际,个人信息权利被当做一项宪法上的基本权利对待,并且,第1条明确规定了本法的立法依据是宪法。这种处理方式既体现了个人信息权利作为一项新型权利的特点和内在要求,也有利于相应的后续信息化法律制度建设。在我国宪法中,可以直接作为本法依据的条款包括第38条、第39条和第40条。另外,诸如宪法第41条、第47条、第51条和宪法修正案第24条,则可以作为本法的间接依据。

第六,关于法律的适用范围

个人信息保护法的适用范围是各国立法时都必须解决的一个重大问题。它主要涉及两个方面的判断或选择:第一是公共部门与私营部门的选择,第二是计算机处理信息与手动处理信息的选择。[21]

对于第一个问题,各国或地区立法模式的差异比较大。既有一部法律不加区别地适用于公共部门与私营部门的(如欧盟指令、欧洲理事会协定、奥地利、波兰、阿根廷),也有在一部法律中分章规定公共部门与私营部门的(如德国和我国台湾地区),也有通过不同法律分别规定公共部门与私营部门的(如日本分别制定的《个人信息保护法》、《关于保护行政机关所持有的个人信息的法律》和《关于保护独立行政法人等所持有的个人信息的法律》,丹麦在2000年7月之前的《1978年公共机关登记法》和《1978年私营机构登记法》),还有一部法律只适用于公共部门的(如韩国、美国[22])。

从个人信息保护的角度来看,不论是公共部门还是私营部门,只要掌握大量的个人信息,均存在滥用或侵犯个人权利的可能。尤其在信息通信技术高度发达、个人信息的收集和处理成本越来越低的环境下,这种可能性只会越来越大。因此,我们认为,从理论上讲,实际上不存在所谓选择问题,个人信息保护法必须同时适用于公共部门与私营部门,以加强对个人权利的保护。因此,从大部分国家的立法情况看,其选择的均是不加区别地将法律适用于公共部门与私营部门。

少数国家或地区之所以在法律的适用范围上有其他的处理方式,我们认为主要是因为两个方面的原因:一是

21 在极少数国家,还可能涉及第三个选择,即个人信息与法人信息的选择,如阿根廷。

22 美国《1974年隐私权法》适用于联邦行政机关,同时,还针对某些领域相继出台了1984年的《有线通信政策法》(Cable Communications Policy Act of 1984)、1986年的《电子通信隐私权法》(Electronic Communications Privacy Act)、1998年的《儿童在线隐私保护法》(Children's Online Privacy Protection Act of 1998)等。

考虑各自法律体系的特点。例如,在大陆法系国家,由于存在公法与私法的划分,公共部门与私营部门传统上适用不同的法律规则,不便于在一部法律中同时规定公共部门与私营部门的法律义务。即使规定在一部法律中,也应分章区别加以规定。这种考虑在德国、韩国、日本与我国台湾地区的立法中体现得比较明显,制度设计的效果也比较好。二是考虑法律规制的强度。一些国家或地区认为,为了保持信息的有效流动,提高企业的效率,实现个人信息保护与经济发展的平衡,对企业的规制不能太多,更多地应通过市场机制或者行业自律机制解决问题。比如,在美国,联邦隐私权法就只适用于联邦政府,而且,美国也没有打算制定一部一般性的个人信息保护法。另外,在韩国,对于私营部门,政府制定了指导性的指南,供其处理个人信息时参考适用。

在专家建议稿中,对于这个问题,我们采用的是统分结合的方式,既有平等适用于公共部门与私营部门的规定,又分章规定了对政府机关与其他个人信息处理者不同的义务。这种处理方式主要是考虑到如下几个方面的因素:(1)从立法资源有限性的角度看,我国现阶段很难对个人信息保护分别制定几个法律,以分别适用于不同的主体。因此,与其因为立法技术上的原因而拖延整个立法的进程,还不如通过制度设计尽快启动个人信息保护立法。(2)统分结合的方式虽然和近年来我国的行政法单独立法方式有比较大的区别,使一部法律中既涉及行政法律关系,又涉及平等主体之间的民事法律关系,使个人信息保护法在归入哪个部门法问题上出现不确定性。但是,应该看到,任何一部法律中实际上都涉及公法与私法两个方面的法律关系,要使法律关系纯而又纯是很难的。不应该根据部门法的理论分类来决定法律的内容和范围。更重要的是,这种统分结合的方式可以有效地利用我国现有的行政法与民事法律救济机制,解决法律的执行问题。(3)从

我国目前所面临的实际问题来看,尽管主要的问题是政府机关掌握的个人信息过多甚至不准确、个人无法获知,但是,与此同时,其他个人信息处理者处理个人信息所造成的问题也越来越多,尤其是一些跨国企业,利用其信息优势牟取不当利益或竞争优势的事例也开始出现。因此,制定一部既适用于政府机关,又适用于其他个人信息处理者的法律,具有多方面的重要现实意义。(4)其他国家或地区已有类似的立法例(如德国、我国台湾地区),实践中证明其是可行的。(5)这种立法模式并不是一成不变的,有较强的适应性。随着立法资源"瓶颈"制约因素的消失,如果需要,以后完全可以从统分结合的方式向完全的分别单独立法方式过渡,对不同主体制定不同的法律。

同时,对于政府机关,专家建议稿采用的基本上是行政复议法与行政诉讼法所调整的主体范围,即除国家行政机关外,还包括其他行使行政管理职能或者提供公共服务的行政主体,如具有行政管理职能的行业协会、公用事业单位、事业单位以及基层群众自治组织等。因此,确定某一主体是否属于政府机关范畴,除依据国家行政机关的形式标准外,某些情况下还要依据其是否行使行政管理职能或者提供公共服务的标准。只要具备行使行政管理职能或者提供公共服务两个标准中的任何一个,都足以构成政府机关的实质条件。当然,鉴于行政复议与行政诉讼中行政主体的范围一直不是非常明确,这一规定在实施中还要根据个案逐步明确其适用范围。换句话说,政府机关的范围具有一定程度的伸缩性或者灵活性,需要在实践中加以明确。当然,即使某些主体经过判断不属于政府机关,仍可以将它归入"其他个人信息处理者",同样需要受到本法的规制。

根据专家建议稿的规定,政府机关的范围是相对较窄的,不包括诸如立法机关和人民法院、人民检察院等司法机关。之所以做这种限定,主要是因为救济机制的制约。

如果将这些国家机关均纳入“政府机关”范畴,就无法适用现行的行政法律救济制度,进而会影响整部法律的实施效果。同时,就实际情况看,大量处理个人信息的主要是行政机关,立法机关所处理的个人信息比较少,司法机关所处理的个人信息要么因为涉及案件的审理而不能公开,要么可以通过审判公开制度或检察公开制度予以解决,因此,将个人信息保护法的主要调整对象集中在行政机关是有道理的。如果实践证明确有必要对立法机关与司法机关的个人信息活动加以规定,也可以参照个人信息保护法,另外制定单行规定。

对于其他个人信息处理者,专家建议稿采用的是比较宽泛的界定。只要是根据个人信息保护法的规定进行个人信息处理的个人、法人或者其他组织,都属于其他个人信息处理者,都平等地受法律的制约。之所以将个人也纳入法律的调整范围,主要的考虑是:(1)与各国通例保持一致,因为几乎所有的域外立法均将个人纳入法律的调整范围。(2)信息通信技术的发展,尤其是互联网的普及,使个人可以低成本地从事个人信息处理活动。如果对这些活动不加规制,会使个人信息权利面临极大的威胁。(3)我国新修订的合同法早已承认自然人的独立法律地位,将个人纳入法律的调整范围不存在任何法律障碍。

对于第二个问题,大部分国家和地区均选择个人信息保护法同时适用于计算机处理信息与手动处理信息,个别的国家或地区则只适用于计算机处理信息(如韩国、我国台湾地区[23])。之所以存在这个选择,是因为始自20世纪70年代世界范围内的个人信息保护立法浪潮直接与信息与计算机技术的出现和普及相关。由于计算机技术的发展,使个人信息的大规模收集和处理成本迅速降低,提高了政府的行政管理效率和企业的竞争力。但是,这种大规模的个人信息处理同时也就蕴涵着对个人信息加以滥用

[23] 我国台湾地区已于2004年9月8日通过修改“个人数据保护法”的“内阁”决定,准备将法律的适用范围扩大至非计算机处理的个人信息。

的巨大风险。因此,个人信息保护法制定之初,其主要立法宗旨就是要解决计算机处理个人信息所带来的巨大风险问题,处理好技术进步与个人权利保护之间的关系。在一些国家或地区的立法中,甚至法律的名称也直接带上了诸如"计算机处理"或"自动处理"的界定,体现了这种立法的时代特征。同时,各国或地区在立法时,为切实保护个人权利,普遍扩大了法律的调整范围,在主要规范计算机处理信息的同时,将传统的手动处理信息的方式也包括在法律的调整范围之内。因此,个人信息保护虽然是计算机时代引出的新问题,但它同时也带动了对传统方式的信息处理活动的规范。

在专家建议稿中,对于这个问题,我们采用了大多数国家或地区的通行做法,明确规定法律同时适用于计算机方式处理的信息和手动方式处理的信息。在我国,由于文字和档案管理制度历史久远,加之许多个人信息处理仍未完全实现计算机化或者自动化,明确法律适用于手动方式处理的信息,不但可以减少法律适用的模糊区域,防止规避法律的现象大量出现,而且,对于真正保护个人权利也具有重要的现实意义。当然,专家建议稿在这个问题上也参考了域外立法的普遍做法,将手动方式处理的信息限制在"根据一定的编排标准或检索方式"进行处理的个人信息,而不是所有的手动处理信息。这样的限定对于降低立法的社会成本,提高执法的有效性,切实保护个人的信息权利,都具有重要的意义。

第七,关于法律的适用例外及其规定方式

几乎在所有的国家,个人信息保护法都有适用例外的情况存在,即在某些法定情况之下,个人信息保护法的规

定全部或部分不予适用。因此,从法理上看,法律的适用例外实际上是法律适用范围的一个必然延伸,两者之间有内在的逻辑联系。

法律之所以规定适用例外,原因是多方面的:首先,由于信息社会涉及大量的个人信息处理活动,法律不可能全部加以规制,否则,不但执法的成本巨大,也会给社会生活造成不便,影响信息的正常流动和交换。因此,各国法律的普遍原则是只规制可能给个人权利造成侵害的信息处理行为,对于不太可能造成权利损害的行为(如个人生活中的信息处理)则不加规制,以实现法律的良好社会效果。其次,个人的信息权利或隐私权利不是绝对的,在保护个人信息权利的同时,还要保护他人的权利(如知情权、言论自由权、科学研究的自由)和社会的公共利益(如统计的需要)。因此,各国均在法律中尽量保持个人信息权利与他人的权利和自由以及社会公共利益之间的平衡。尤其是公众的言论自由权和科学研究的自由,往往是法律重点加以保护的领域,许多情况下都被作为例外处理,因此不得以保护个人信息为由妨碍言论自由权和科学研究的自由。再次,国家安全问题在现代社会一直占据着重要的地位,尤其是近年来恐怖主义的猖獗更使国家安全成为各国政府必须正视的重大问题。为了保证国家安全,必须授予执法机关一定的权力和手段,以发现和惩处犯罪分子,为此,个人甚至不得不做出一定的牺牲。在许多国家的个人信息保护法中,均将国家安全作为一项常见的适用例外加以排除,以保证执法机关的执法活动不受外界的干预和影响。

尽管各国对于法律适用例外的范围规定不尽一致,有的范围较广,有的范围较窄,有的采用高度概括的方式加以规定(如欧洲理事会协定第9条、欧盟指令第3条),有的采用具体列举的方式加以规定(如荷兰个人数据保护法第2条第2款、日本个人信息保护法第50条、冰岛个人数据保护法第5节、瑞典个人数据法第7节)。但是,其范围

覆盖的基本是国家安全、新闻出版、科学研究、统计活动、纯粹个人的信息处理活动等方面。并且,在规定的方式上也基本可以分为两个层次:第一层次是完全排除,第二层次是适用限制。所谓完全排除,是指对于某些领域或者事项,个人信息保护法根本不予适用,一般规定在法律的总则部分。所谓适用限制,是指对于某些领域或者事项,虽然应该适用个人信息保护法,但法律同时给予其豁免或适用限制的地位,减损个人信息保护法的法律效力,一般规定在法律的分则部分。

上述两种规定方式的差别体现在许多方面:首先,它们各自在法律结构中的位置不同,前者大部分规定在总则部分,后者则规定在分则部分;并且,就法律适用例外的强度而言,前者比后者要大。其次,前者主要适用于诸如国家安全等领域或事项,而后者主要适用于诸如医疗、新闻出版、文学创作等领域。再次,前者可以说是某种事先机制,其范围相对比较清晰,已经根据一定的标准进行了事先的排除,具体个案中自由裁量权的范围不大;而后者可以说是某种事后机制,其范围要模糊得多,并没有进行事先的排除或限制,可能需要适用机关在个案中运用自由裁量权明确其具体范围,进行利益权衡。最后,前者的标准相对比较单一,根据具体领域的性质统一划定界限;后者的标准则体现了多元性的特点,要根据具体的问题或者事项,分别设计相应的限制条件和标准。

当然,尽管有上述差别,但两者之间的界限又不是绝对的。这主要表现在两个方面:一是不同的国家或地区的法律对于相同的领域或事项(如刑事犯罪侦查)完全可能做不同的处理,既可以作为第一层次完全排除,也可以作为第二层次适用限制。二是即使在同一个国家,随着形势的变化,对相同的领域或事项也完全有可能做不同的处理,两者之间的特征也会发生一定程度的相互融合。因此,在这个问题上,各国最为重要的经验是,只有综合运用事先与事后两

种不同的适用例外机制,既有完全排除的事项,又有适用限制的事项,才能妥善地处理好个人权利与他人权利和社会公共利益之间的关系,实现法律的良好社会效果。

在专家建议稿中,我们充分吸收和借鉴了各国在两种机制设计上的经验,在第一章总则部分规定了统一的事先完全排除机制,在随后各章(主要是第二章、第三章)规定了多元化的事后适用限制机制。我们认为,这种规定方式的好处在于:首先,通过第一层次的事先完全排除,可以免除人们对国家安全问题的担忧,扫清个人信息保护法立法中可能遇到的阻力;实质性地减少法律的覆盖范围,降低执法成本;为将来制定实施细则提供法律依据,协调好个人信息保护与信息的自由流动之间的关系,防止法律的社会成本过高,影响社会的发展。其次,通过第二层次的事后适用限制,可以针对具体问题,在实践中平衡个人信息保护与其他权利之间的关系,保持法律的灵活性和必要的张力。再次,不论是第一层次的事先完全排除还是第二层次的事后适用限制,专家建议稿在制度设计和措辞上都保留了相当的弹性,使两个层次之间能够在形势发展变化以后,在实施中相互融合、配合和转化。

对于第一层次的事先完全排除,专家建议稿规定了三种类型:一是不适用于国家安全机关为保障国家安全而进行的个人信息处理,其具体范围由国务院决定。[24] 二是不适用于公民在纯粹的个人或家庭活动中所进行的个人信息处理。三是不适用于法人或其他组织数量较少,且不太可能对个人权利造成侵害的个人信息处理活动,其范围由国务院信息资源主管部门通过制定规章确定。对于前两类,标准比较明确,争议不大,滥用的可能性也较小。对于第三类,起草过程中,有比较多的不同意见。许多同志认为,该类排除标准不明确,缺乏严格的程序制约,授予国务院政府信息资源主管部门的权力过大,有可能被滥用。经过非常慎重、反复的考虑,并且充分认识了不同意见的合

[24] 只是排除这类活动适用个人信息保护法,并不排除其他法律可能对这类行为的规定。

理性,专家建议稿仍决定保留该类排除,理由在于:(1)我国个人信息保护制度处在刚刚起步阶段,配套的社会环境和相关制度均不够完善,全社会对这个领域都不太熟悉,因此,个人信息保护法很难像某些域外立法那样进行全面详细的列举(如明确排除基于新闻、艺术和文学目的而进行的个人信息处理)。详细列举的好处在于标准明确,但其弊端在于使法律缺乏适应性。对于刚刚启动个人信息保护工作的我国而言,保留法律的一定弹性,对于制度的尽快启动、实施和降低立法的社会成本具有十分重要的意义。因此,保留本类排除,与其说是一种选择,不如说是没有选择的选择更合适。(2)本类排除虽然授予国务院信息资源主管部门较大的权力,但这种权力的行使是有条件的,必须通过正式的、制定规章的形式确定,其他任何形式均不符合法律的规定。(3)随着个人信息保护工作的逐步开展和配套制度改革的到位,涉及本类排除的事项必然会通过单行立法提升规范法律的位阶,使国务院信息资源主管部门通过规章确定的范围逐步缩小,限制行政权力。(4)如果专家建议稿所设想的独立信息委员会能够设立,可以实质性地增加政府决策的公开性、民主性与科学性,减少权力滥用的可能。(5)在我国现行法律结构之下,对国务院部委制定规章行为本身已经存在多种监督制约机制,包括立法、行政与司法监督,因此,只要这些制约机制能够充分发挥作用,应该可以有效防止权力的滥用。

第八,关于个人信息处理的基本原则

为有效保护个人信息,同时,也为了便利信息的有序流动,许多国家或地区的个人信息保护法均规定了一些基本原则,用以指导个人信息处理活动。经合组织指南规定

了八项原则,分别是:(1)收集限制原则。个人数据的收集应该受到限制,任何此类数据的获得都应该通过合法和公正的方法,在适当的情况下,要经过数据主体的默示或同意。(2)数据质量原则。个人数据应该与它们将要被使用的目的和该目的所需要的程度相关,个人数据应该精确、完整和被保持为最新状态。(3)列明目的原则。收集个人数据的目的应该在数据收集之前列明,并且随后的使用应限于实现这些目的,或者那些和前述目的并非不相容的目的,这些情况应当在其目的改变时列明。(4)使用限制原则。除非经过数据主体的同意,或者经过法律的授权,不应该在列明的目的之外披露或公开使用个人数据。(5)安全保护原则。个人数据应该受到合理的安全保护,以免被丢失或未经授权而被获取、破坏、使用、修改或披露。(6)公开原则。应该制定关于个人数据的发展、实践和政策的一般的公开政策。应该确立便利的措施,以确定个人数据的存在和性质,它们使用的主要目的,以及数据控制者的身份和通常住所。(7)个人参与原则。个人应当有权利从数据控制者那里获得或者确认数据控制者是否拥有有关他的数据;如果其要求被拒绝,他有权获知理由,可以挑战此拒绝;如果这一挑战成功,他可以删除、纠正、补充完整或修改这些数据。(8)责任原则。数据控制者有责任遵守赋予上述原则以效力的措施。

欧洲理事会协定规定的基本原则包括如下七个方面,分别是:(1)数据质量,被自动化处理的个人数据应当:a正当合法地获取和处理;b 基于特定的合法目的存储,并不得以与这些目的相悖的方式被使用;c 与存储的目的具有充分、相关而不多余的关系;d 是准确的,并在必要时保持更新;e 通过允许识别数据主体的方式被保存,但保存时间不得超过存储数据所必需的期限。(2)数据的特殊类型。除非国内法已提供了适当的保护措施,禁止对揭示以下内容的个人数据进行自动化处理:人种、政治主张、宗

教或其他信仰以及与健康或性生活有关的个人数据。与刑事判决有关的个人数据,也不应当被自动化处理。(3)数据安全。应当采取适当的安全措施,保护自动化数据文档中的个人数据,使其免受偶然或未经授权的破坏或意外丢失,同时免受未经授权的获取、变更或分解。(4)对数据主体的保护,应当使任何人能够:a 确认自动化个人数据文档的存在,获悉文档的主要目的、文档管理者的身份、惯常居所及其主要营业地;b 在合理的期限内、无过多延迟、无过多花费地确认与其相关的个人数据是否已被存储在个人数据文档中,以及通过能被其理解的方式向其传达这些数据;c 如果被处理的数据违反了法律的规定,则可以对这些数据进行矫正与删除;d 如果没有满足数据主体关于本条 b 款和 c 款规定的确认、传达、矫正或删除数据的要求,则数据主体可以要求赔偿。(5)例外与限制。对个人数据保护的例外或限制必须是基于以下目的并且采取在民主社会中必须采取的措施:a 保护国家安全、公共安全、国家的财政利益或抑制刑事犯罪;b 保护数据主体或他人的权利和自由。(6)赔偿责任,对违反有关数据保护基本原则的行为,应当承担适当的制裁措施与赔偿责任。(7)扩大的保护。关于个人数据保护,本法所有的规定都不得被解释为是对一方授予数据主体超过本法规定之更多保护措施的限制或其他影响。

其他国家或地区的立法所确立的基本原则大致上都在上述这些原则的范围之内,但也有的国家在此基础上确立了一些更进一步的原则,比如德国的联邦数据保护法第 3a 条就确立了“信息缩减与信息节约”的规定,要求信息处理系统尽可能不采用或者采用最少量的个人信息,而且,应尽可能采用匿名的个人信息。同样,美国专门制定了公文削减法,要求政府机关收集信息尽可能降低社会的成本。卢森堡所制定的数据保护法律的名称为《关于计算机处理中最少使用数据法》,体现了政府机关信息收集活

动尽量减少社会成本的立法意图。

各国或地区究竟采用哪些基本原则,很大程度上取决于对个人信息保护的不同认识。由于各国的国情不同,对个人信息保护的方式有差异,对不同价值之间的关系排序未必一致,因此,法律采用的基本原则的范围和强度都是有差别的。有的法律规定的基本原则非常广泛、全面,或者容许例外或限制的情况非常少;有的法律则只侧重规定某些方面的基本原则,如禁止滥用、对信息主体公开,或者规定比较广泛的例外或限制。这是各国或地区法律中对于基本原则问题上的差异之处。但是,此外,域外立法在基本原则问题上也有相同之处,那就是基本原则覆盖的主要是个人信息处理过程中的三个主要环节,即信息的收集、信息的使用与信息主体对个人信息的权利。这种同与异的并存,使个人信息保护法律既有多样性,又有普遍性。

在这个问题上,专家建议稿充分辨析、吸收、借鉴了域外立法的经验,同时,考虑到政府机关与其他个人信息处理者在信息处理法律性质上的根本差异,考虑到我国立法实践中区分总则与具体章节的特点,因此,决定将个人信息处理的基本原则分解到总则与具体章节之中。总则部分规定了政府机关与其他个人信息处理者必须共同适用的原则(七项),第二章、第三章则针对政府机关与其他个人信息处理者的不同法律地位,分别规定了相应的原则或行为规范,供其遵守。总体上看,专家建议稿所规定的基本原则基本上覆盖了域外个人信息保护法所确立的基本原则,只是在敏感信息的处理上,并未明确予以规定。

第九,关于本法与政府信息公开条例的关系

尽管个人信息保护与政府信息公开是两项不同的制

度,两者绝对不是一回事。但是,由于个人信息保护法所规范的一个重要部分是政府机关所持有的个人信息,因此,个人信息保护法必然与政府信息公开法发生部分重叠,两者之间有内在的必然联系。仅就政府机关而言,个人信息保护与政府信息公开在许多情况下可以说实际上是同一个问题的两个方面。

在国际社会,个人信息保护与政府信息公开之间的这种联系,主要体现在两个方面:一是立法上,二是执法机制上。在一些国家,立法上就采取了两法合一的形式,将个人信息保护与政府信息公开规定在一部法律之中。例如,匈牙利 1992 年制定的《个人数据保护与公共利益数据公开法》,俄罗斯 1995 年制定的《俄罗斯联邦信息、信息化与信息保护法》,南非的《信息公开促进法》,泰国的《官方信息法》,都同时规定了政府信息公开与个人信息保护制度,实现了程度不同的两法合一立法模式。在另外一些国家,虽然没有采取两法合一的立法模式,但在执法机关(尤其是执法机关)上实现了两个制度之间的统一和整合,由一个共同的机构或者机关来负责两个制度的实施。例如,美国司法部信息与隐私办公室负有推动政府信息公开与个人信息保护的双重责任,日本信息公开与个人信息保护审查会作为高层次的机构,实现了多部法律执法机制的统一。我们认为,不论是立法合一还是执法机制的统一,其好处都在于可以节约资源,使两种制度相互促进。尤其是当两个制度发展不平衡时,采取相互联系的立法方式或者执法机制,可以使发展较弱的制度获得外在的推力,促进其共同发展。当然,当制度发展比较成熟以后,两种制度相互之间的需要可能不再那么强烈,制度的分化与分离也许更有利于各自独立发展。

在我国,由于政府信息公开与个人信息保护制度均处在起步阶段,两部法律的立法过程都存在较大的不确定性。在这个阶段,加强两者之间的联系,使任何一点的突

破都能够为另外一点带来助力,具有重要的战略意义。因此,在我们先期起草的《政府信息公开条例》(专家建议稿)中,就考虑到了政府信息公开与个人信息保护制度的衔接问题,并在法规草案中确立了个人信息保护的原则。尽管从理论上讲,完全可以将政府机关的个人信息保护的所有内容全部规定在政府信息公开条例之中,使个人信息保护法只适用于其他个人信息处理者。但是,考虑到两个制度的性质差异,考虑到两个制度的推进步伐不可能相同,并且,考虑到政府信息公开制度即使能够及时推进,也仍停留在行政法规的层面,而个人信息保护由于涉及个人基本权利,显然不适宜由行政法规规定,因此,《政府信息公开条例》(专家建议稿)只是非常简单地规定了个人信息保护的基本原则,没有进一步规定具体的操作标准与程序。

起草本法时,尽管政府信息公开条例仍未通过,但是,基于同样的战略考虑,专家建议稿对个人信息保护与政府信息公开制度的衔接给予了特别的关注,并通过三种方式来加强两者之间的衔接:一是第二章第二节关于信息主体获得个人信息权利的程序规定,尽量与政府信息公开条例的规定保持一致和衔接;二是两部法律草案规定的政府信息资源主管部门均是同一个执法部门;三是两部法律草案均设计了一个非常设、中立、独立的信息委员会,以保障制度的有效性,也符合国际社会的一般要求。我们认为,这样的处理方式,不但可以避免因为两个制度不同步、两部法律效力等级不同可能会导致的不一致或冲突,并且,不论哪一部法律先出台,均有利于带动另一个制度。更为重要的是,通过整合有限的行政执法资源,形成局部优势,有利于在执法实践中推动两个制度的发展。

第十,关于对政府机关与其他个人信息处理者的不同规制方式及其效果

在国际社会,这个问题与法律的适用范围问题密切相关。如果个人信息保护法同时适用于政府机关与其他个人信息处理者,就必然会产生一个对两者的规制方式与程度是否应该相同这样的问题。一般而言,如果个人信息保护法不加以区别地适用于公共部门与私营部门,则其规制方式与程度大致相同;如果个人信息保护法分章规定公共部门与私营部门,或者分别立法以分别适用于公共部门与私营部门,则其规制方式与程度会体现明显的差别。

由于专家建议稿采用的是分章为政府机关与其他个人信息处理者分别设立行为规范的立法方式,因此,在规制的方式与程度上存在比较明显的区别,对政府机关的规制程度要弱于对其他个人信息处理者的规制程度。这主要是因为,政府机关处理个人信息是其履行法定职责、实施行政管理的必然要求,从法律性质上看属于行政法律关系。相反,其他个人信息处理者处理个人信息是一种民事主体的自主活动,从法律性质上看属于民事法律关系。由于法律关系的性质不同,决定了对其不可能采用同样的规制方式。当然,对政府机关的规制程度弱于对其他个人信息处理者的规制程度,只是就原则而言的,并不意味着在每一个制度设计上都是更有利于政府机关的个人信息处理活动。实际上,政府机关除了遵守个人信息处理的专门法规范以外,还要遵守作为行政管理者的一般行政法规范。从这个意义上讲,对政府机关的规制程度显然又要远远强于对其他个人信息处理者的规制程度。

尽管规制方式不同,我们认为,专家建议稿的制度设

计能够达到保护个人信息的立法目的。

对政府机关而言,确保规制有效性的主要措施在于:(1)尽管政府机关可以在其法定职权范围内为履行其职责收集个人信息,但这种收集活动必须有明确、合法和特定的使用目的;另外,收集个人信息,不得超出实现使用目的的范围;并且,收集个人信息应尽可能减轻社会负担,避免重复收集个人信息。(2)政府机关在开始收集个人信息之前,应就有关事项向各级人民政府信息资源主管部门进行登记,履行登记义务。(3)登记事项必须公告,这既方便了公众查询个人信息,又可以在无形之中形成对随意收集个人信息行为的制约。(4)政府机关只能在收集个人信息时所明确地使用目的范围内处理个人信息,如果超出这个范围进行处理,必须符合严格的限制条件,这样,可以有效地防止个人信息被滥用。(5)通过赋予个人行使获得个人信息的权利,可以防止政府机关违法进行个人信息的处理。(6)通过救济机制的设计(包括政府信息资源主管部门统一受理行政复议案件,条件合适时设立独立的信息委员会等),保证政府机关依法进行个人信息处理活动。(7)明确政府机关的赔偿责任,追究其违法行为。(8)明确规定政府机关直接责任人和相关负责人的行政责任,提高其依法行政的自觉性。(9)明确规定政府信息资源主管部门工作人员的责任,以建立有效的执法保障机制。

对于其他个人信息处理者而言,确保规制有效性的主要措施在于:(1)专家建议稿明确规定,除符合几种严格的法定条件外,其他个人信息处理者不得进行个人信息处理。并且,其他个人信息处理者必须通过合法、正当的方式收集个人信息。这些规定可以防止个人信息收集环节上的失控。(2)其他个人信息处理者开始进行个人信息收集之前,须向政府信息资源主管部门进行登记,或者须经政府信息资源主管部门行政许可,政府信息资源主管部门分别进行形式审查和实质审查,由此可以保证对个人信

息收集的政府监督。(3)政府信息资源主管部门的登记或许可决定需要予以公告,供公众查阅。其他个人信息处理者需要将登记或许可事项制作个人信息文件登记簿,供公众查阅。这样,可以形成对个人信息处理的公众监督。(4)其他个人信息处理者收集或处理个人信息必须有明确、特定的使用目的。超出特定的使用目的处理个人信息的,必须经信息主体事先同意。由此可以防止个人信息的使用泛滥。(5)其他个人信息处理者直接自信息主体收集其个人信息时,应将有关事项告知信息主体,由此保证信息主体的知情权和选择权。(6)符合条件的,政府信息资源主管部门可以限制跨境个人信息传输,这样既可以维护国家利益,也可以保护信息主体的权利。(7)通过赋予个人获得个人信息的权利,可以防止其他个人信息处理者违法进行个人信息处理。(8)通过救济机制的设计(包括投诉机制、行业自律机制和行政管理机制),可以保证其他个人信息处理者迅速解决争议,依法进行个人信息处理活动。(9)通过明确各种形式的违法行为(包括未经登记或许可进行个人信息处理)的法律责任,确保个人信息保护法的规定能够得到实施。

第十一,关于协调个人信息保护与促进信息自由流动的关系

个人信息保护法一方面需要保护个人权利,同时,另一方面,又不能阻碍正常的信息流动,加大市场主体的交易成本,阻碍社会的进步。尤其在信息时代,信息作为战略性资源,其自由流动具有重要的基础性意义。如果对个人信息的保护走入极端,势必使每一个人都成为一座“信息孤岛”,全社会成为一盘散沙。因此,如何协调好保护个

人信息与促进信息自由流动的关系,可以说是各国立法当中最为重视的一个问题。对这个问题的不同回答,也就决定了诸如是否立法、如何立法、法律的规制程度如何这样的问题。在这一对价值中,偏废任何一个方面,都是不足取的。

在国际社会,个人信息保护法均突出强调了协调好两者关系的极端重要性。例如,欧洲理事会协定在导言部分明确提出:"考虑到遭受自动处理之个人数据越来越多地跨国流动,由此应当扩大对大众权利及其基本自由的保护,尤其是对隐私权的尊重;同时重申成员国无论国界而保证信息自由流通之承诺;承认必须在遵守隐私的基本价值和尊重信息在国家间自由流动两者之间达至平衡。"经合组织指南在导言部分规定:"在隐私和个人自由的保护方面,在协调诸如隐私和信息的自由流动这些基本的但却冲突的价值方面,成员国有着共同的利益;成员国应该努力消除或避免以隐私保护的名义为个人数据的跨疆界流动制造障碍。"欧盟在说明制定共同的数据保护指令的原因时指出:"为了消除个人数据流动中的障碍,各成员国对个人数据处理中个人的权利和自由的保护措施必须相同;各成员国对于个人权利和自由特别是隐私权,在个人数据处理过程中不同程度的保护措施可能会阻止这些数据在成员国之间的传送;这些差异因此可能对许多欧共体的经济活动形成障碍、扭曲竞争并阻止各国政府履行欧共体法律所规定的责任。"同时,欧盟指令第 1 条明确规定:"各成员国应对个人数据处理中自然人的基本权利和自由,特别是他们的隐私权予以保护。各成员国不应限制或禁止出于与第 1 款所提供的保护有关的原因,而在各成员国之间所进行的个人数据的自由流动。"

为协调这一对价值,域外立法在制度设计上可谓煞费苦心。各种不同的选择主要体现在保护的模式、法律原则的范围与具体的制度设计等方面。

根据国际上对隐私的研究,各国或地区对个人信息的保护,主要有四种模式。根据不同环境,这些模式之间可以是相互补充的关系,也可以是相互冲突的关系。绝大多数国家,都是同时使用几种不同的模式。对个人信息保护最为有效的国家,会使用所有的模式,以加强对个人信息的保护。

综合立法模式

世界上许多国家都制定一部一般法,规范公共机关与私营部门对个人信息的收集、使用和传播等活动,同时,会有一个监督机构负责法律的实施。采用个人信息保护法律的大多数国家都倾向这种模式,欧盟也采用了这种模式以保障其数据保护体制的有效性。加拿大与澳大利亚采用了这种模式的某种变种,被称为"共同管制模式",即由商界制定并负责实施保护隐私的规则,隐私管理机关负责监督。

特别立法模式

某些国家,如美国,避免制定一般性的数据保护法律,而是倾向制定特别法,调整诸如租借录像记录、金融隐私等特定的问题。[25]在这种模式之下,个人数据保护需要通过一系列的机制加以实施。这种模式的缺陷在于,它往往需要新的立法来赶上每一种新出现的技术,因此经常造成法律的相对滞后。美国对互联网上个人隐私缺乏法律保护就是一个典型的例证。同时,在这种模式之下也没有一个统一的监督机构。在许多国家,特别法常常被用来补充综合立法,为诸如通信、警察档案或者消费者信用档案等种类的信息提供更为详细的保护。

㉕ 美国首先于1970年制定了《公平信用报告法》,要求收集消费者信用信息并向有关企业提供的"消费者信用报告机关"采取合理措施对消费者个人信用信息、人事信息等予以保密并保证其正确性。为了保护公民隐私权不受联邦政府各种行为的侵害,美国于1974年出台了专门针对联邦政府部门的《隐私权法》。该法是联邦政府部门个人信息保护的基本法规,意在确立联邦政府保护个人信息的义务。美国没有一部全国通行的综合性的隐私权保护法律,由各个联邦法律组成的综合法包含了一些详细的个人信息种类,包括财政记录、信誉记录、录像租金、有线电视、儿童的(13岁以下)网上活动、教育记录、机动交通登记和电信市场。在个别法方面,美国相继出台了1984年的《有线电视通信政策法》、1986年的《电子通信隐私权法》、1998年的《儿童在线隐私权法》等。在非政府部门方面,很重要的一项措施便是实行第三方认证制度,即由第三方向采取适当的个人信息保护措施的企业授予隐私标识。从事这一活动的民间组织有BBBonline、TRUSTe、CPA WebTrust等。

自律模式

至少在理论上,个人信息保护也可以通过各种自律机制实现。在这种模式下,业界制定行为规范并进行自律。不过,在许多国家,尤其是美国,这些努力的效果并不令人满意,能够表明行为规范的目标实现的证据很少。这种模式的主要问题存在于保护的充分性和可执行性上,业界制定的规范在许多国家只能提供非常微弱的保护,并且缺乏执行手段。[26]

技术保护模式

随着商用技术的发展,个人使用者也开始可以保护个人隐私。因特网和某些物理应用程序的使用者可以采用提供隐私与通信安全保障的各种程序与系统,包括加密技术、匿名重发邮件、代理服务器以及数字货币等,保护个人隐私。这种模式的问题在于,并非所有的工具都能有效地保护个人隐私。有些程序设计粗糙,有些则可能是为了便利执法部门获取信息。

如果说上述四种模式表明各国或地区在个人信息的保护模式上还基本有章可循的话,那么,在个人信息保护立法原则、制度的选择上则可谓百花齐放、异彩纷呈。可以将保护个人信息与促进信息的自由流动当做一个区间的两端。域外个人信息保护立法,几乎就每一个原则、每一项制度、每一种例外、每一个程序,在这两端之间都存在着无数的不同选择。各国或地区根据自己的实际情况,都会对如何协调这一对价值给出自己独特的回答。

专家建议稿主要在如下几个方面对协调个人信息保护与促进信息的自由流动进行了考虑。(1)第1条明确规定立法的目的包括"保护个人权利,促进个人信息的有序

㉖ 例如,在日本,1988年就出台了保护中央政府机关电子计算机处理的个人信息的《关于对行政机关所持有之由电子计算机处理的个人信息加以保护的法律》。而对于非政府部门的信息处理,长期以来则没有专门的法律进行规范,主要是通过个别法的某些规定、行政指导和行业自律等措施相互作用进行规制。比如,《职业安定法》第5条之4就规定了职业介绍机构等在保护求职者个人信息方面的责任。通商产业省也曾于1997年3月公布了《关于保护民间部门电子计算机处理所涉及的个人信息指南》,以指导非政府部门的个人信息保护。同时,以1995年欧盟指令的出台为契机,财团法人日本情报处理开发协会开始运作"隐私标识"制度,依据指南向采取有力措施保护个人信息的非政府部门颁发"隐私标识"。但是,由于1988年法律仅适用于政府部门,对于非政府部门则缺乏原则性的统一规定,而且,类似通产省指南的行政指导以及各种自律措施缺乏拘束力,恶意收集、使用或者泄露个人信息的案件时有发生,并且救济和制裁措施也很不完善。为此,日本经过长期讨论,最终又于2003年出台了《个人信息保护法》、《关于保护行政机关所持有之个人信息的法律》、《关于保护独立行政法人等所持有之个人信息的法律》、《信息公开与个人信息保护审查会设置法》以及《对〈关于保护行政机关所持有之个人信息的法律〉等的实施

流动”两个方面,突出法律的双重价值。(2)对个人信息的保护模式采取综合立法、特别立法、自律与技术保护相结合的形式,既制定统一的个人信息保护法,又不排除另行制定特别法和采取自律机制。(3)明确将利益平衡原则作为一项原则加以规定,既保护个人信息,同时也保证其他价值的实现。(4)规定有一定弹性的适用例外,以便在实践中平衡个人信息保护与其他的利益。(5)根据政府机关与其他个人信息处理者,以及其他个人信息处理者之间的性质差别,设计不同的行为规范,避免过度规制。(6)专门设计行业自律机制,并为逐步实现由政府直接管理向行业自律组织管理过渡创造条件。(7)法律文本中未采用许多国家立法中均采用的敏感个人信息概念及其相应的制度,以保持制度的最大弹性。(8)在法律条款的设计与措辞上尽量体现原则性与灵活性的有机结合,以适应各种不同的实际情况。

所涉及的相关法律进行完善等的法律》。其中,《个人信息保护法》针对政府部门和非政府部门规定了保护个人信息的若干共同事项,《关于保护行政机关所持有之个人信息的法律》和《关于保护独立行政法人等所持有之个人信息的法律》则适用于政府部门和行使行政职能的特殊法人。对于非政府部门,则仍主张应尽可能地针对具体情况制定个别法或者加强其自律。

第十二,关于个人信息保护法在特定行业的法律适用问题

协调个人信息保护与促进信息的自由流动的关系,非常集中地体现在特定行业的法律适用上。确立个人信息保护的法制体系、保障公民的合法权益,这是经济和社会发展所必需的。但是,由于不同的行业对个人信息的利用情况各不相同,对所有行业使用划一的规制措施显然会有一定的困难。因此,许多国家普遍对特定的行业研究制定特别的规定。例如,欧盟指令允许为了历史、统计和科学目的而长期储存个人信息(第6条),允许为医疗卫生目的处理敏感的个人信息(第8条),要求调和个人信息处理与表达自由之间的关系(第9条)。个人信息保护法在

以下几个特定行业的适用,尤其具有特别意义。

首先涉及的当数个人信息保护法同媒体活动之间的关系。媒体进行正常的采访和报道乃是一个社会得以健康发展所必需的,是实现公民的知情权,推进政府信息公开的重要保障。采访活动不同于一般的商业往来,它一般情况下必然是单方性的,并极其强调时效性。采访什么内容、如何对所采访的内容加以运用以及如何及时向受众传递各种信息,这些均应当由媒体自行加以判断。如果要求媒体在收集个人信息的过程中必须事前征得本人的同意,直接自本人处获取信息并在其同意的前提下使用该个人信息,那么,媒体必将难以充分发挥其应有的作用。原则上讲,凡是媒体进行报道涉及公共利益的,个人的隐私权均应当受到限制。但是,对于何为公共利益、如何认定报道的正当性并没有恒定的标准。在国外,一般是由司法机关对此进行具体判断,并依据判例形成一定的规则。

日本在制定个人信息保护法的过程中,有关方面就如何处理其与媒体之间的关系问题展开了激烈的争论。2002 年 4 月,日本政府送交国会审议的《个人信息保护法草案》规定设立主管大臣专门对报道机关进行监督;由独立的行政委员会对采访、报道活动进行裁量性审查。当时,媒体对此反应强烈,认为这将导致政府有可能以保障隐私权为由干涉公民的表达自由。[27]日本的立法过程中提出反对意见的主要是媒体,这与忧虑个人信息保护的严格规定会导致媒体的表达自由趋于萎缩不无关系。事实上,各国的个人信息保护法也都注意到协调同媒体等行使表达自由之间关系的问题,都允许其完全或者不完全地排除适用个人信息保护法。[28]

另一个涉及个人信息保护法适用问题的重要领域是征信行业。征信是指以了解企业资信和消费者个人信用为目的而对涉及信用交易的信息进行核实和依法传播的活动,包括企业征信和个人征信。个人征信是指个人信用

[27] 《日本经济新闻》2002 年 4 月 25 日第 1 版。

[28] 比如冰岛《处理个人数据中保护个人法》第 5 节、瑞典《个人数据法》第 7 节,而日本 2003 年 5 月份出台的《个人信息保护法》最终做出了让步,规定有关民间团体处理个人信息时应遵循的规则不适用于媒体为报道行为而处理个人信息的行为。

局根据申请,向合法的用户提供消费者个人的信用记录或者档案,帮助授信机构或者雇主做出正确的授信、赊销和聘任决定。征信业是信用社会必不可少的行业,可以为金融机构、商家等提供可量化的授信参考,有利于推动信用消费的健康发展。同时,征信活动还可以有力地支持失信惩罚机制发挥作用,具有较强的公共性。个人征信的对象是个人的姓名、地址、出生年月、教育背景、工作经历、付款记录、收入、纳税与开销等个人信用信息,其来源是掌握个人信用信息的各种政府机关和各种非政府部门。个人征信的对象、目的与作用决定了其特点,即征集和传播的仅限于与清偿有关的信息。对个人信用信息的征集、传播往往是在被调查对象毫不知情、被动的情况下进行的,除涉及国家秘密等以外,政府部门对于征信局查询个人信用信息的合法的请求应当予以满足。同时,个人信用信息必须及时更新。可以说,征信活动有着某些不同于其他信息处理活动的地方,比如,信息主体对于个人信用信息的传播是否还像其他信息一样享有做出同意的权利就是值得研究的。美国联邦贸易委员会委员长缪里斯曾指出,正是由于个人信用体系的存在,才可使信用较好的消费者在短时间内从毫不认识的人那里借到钱,该体系存在的前提是信用调查机关可以未经任何人允许地获得他人的敏感信息。[29]由于征信业的特殊性,许多国家、地区都对其处理个人信用信息做出了专门的规定。比如,丹麦《个人数据处理法》规定,设立征信机构应当经信息保护专员的授权(第19条);韩国《关于利用与保护信用信息的法律》规定,征信机构的设立应经金融监督委员会批准(第4条)。在所处理信息的范围方面,丹麦的法律规定,征信机构只能处理与其性质相关的评估财务状况和涉及信用程度的信息,不能处理各种敏感的个人信息(第20条);韩国的法律要求征信机构处理涉及个人疾病的信息时,必须经过本人同意,并在总统令规定的限度内予以利用(韩国《关于

[29] [美]巴里·克耐里(Barry. Connelly):"消费者信用:反映美国经济兴衰的晴雨表",载《个人信用信息专刊"i"》(日本刊物)第52号,第12页。

利用与保护信用信息的法律》第15条),而且,个人信用信息的提供、利用仅限于用以判断可否同其主体确立或维持金融交易等的关系(第24条);美国的《公平信用报告法1996年革新法》还依照个人信用信息的合法用途明确了八类合法的用户群。同时,征信机构有义务维持个人信用信息处于最新的状态,并有义务删除旧的、可能给信息主体带来不利益的信息(比如韩国《关于利用与保护信用信息的法律》第18条)。

涉及个人信息保护法适用问题的第三个领域是医疗机构对个人医疗信息的处理。个人医疗信息是与疾病的诊断、治疗相关而产生的个人信息,包括患者的基本信息、健康保险和社会福利方面的信息、生活背景方面的信息、医学背景上的信息、检查结果、治疗过程的记录等。与一般的个人信息相比,医疗信息具有许多特殊之处:在利用目的上,该信息除了被用于患者个人的康复以外,还被用于医学教育、医院管理、医学研究、对其他医师的指导等,可以促进医疗水平的提高和医学的进步,具有公益性;医疗信息既包括对患者病情的客观记录,也包括主治医师思考过程等的主观判断;医疗信息有时不能直接自患者本人处取得,而要从其亲朋以及某些机构处获取;某些医疗信息(比如罹患不治之症,或者患者丧失意识)不便于向患者本人公开;个人医疗信息的保存期间不能"一刀切",对于某些特殊的疾病,为了进行跟踪治疗或者进行医学研究,往往需要较长期间的保存。当然,许多个人医疗信息可以在去除姓名等可识别个人的信息后予以利用。鉴于此种信息的特殊性,对其加以特殊规定是必不可少的。特别是,如果对于医疗信息的收集、利用采取同其他一般信息相同的措施予以管理,很有可能对疾病的预防产生负面影响。以癌症为例,日本实行地方癌症登记制度,而日本《个人信息保护法》出台之后,人们便担心,法律中关于未经本人允许不得向第三人提供其个人信息的规定会导致

癌症登记的精密度下降。[30]

另外,个人信息保护法还有可能对律师业造成一定的影响。如果严格按照经合组织指南确立的八项原则,律师将无从调查取证,正常开展业务。因此,许多域外立法也对此做出了排除性的规定(比如比利时《数据保护法》第8条、意大利《数据保护法》第20条)。与此类似,诸如银行、保险、电信等行业,也都会涉及个人信息保护法的适用问题。

对于个人信息保护法在特定行业的法律适用问题,专家建议稿明确了以下几项原则:(1)只要法律没有明确规定完全排除或限制适用,对个人信息保护法的规定均应平等地加以适用;否则,法律权威无法维护,规避法律的行为会大量产生。(2)国务院信息资源主管部门可以制定规章,对某些特定行业全部排除个人信息保护法的适用或者做出适用限制。(3)如果单行立法另行做出其他规定,包括做出比个人信息保护法更为严格的规定,应优先适用特别法的规定。之所以在专家建议稿中没有具体规定任何特定的行业,是因为我国在个人信息保护方面还没有经验,并且,这些行业在我国有其不同于国外的特点,不宜简单照搬域外的立法经验。我们认为,目前这种处理方式既可以较好地保护个人信息,又可以根据实践的需要,促进信息的有效流动。

第十三,关于敏感个人信息问题

敏感个人信息保护是域外立法当中的一个重要领域,其目的是对某些特殊种类的个人信息给予更高程度的保护,防止个人权利受到侵害。例如,欧洲理事会协定第6条明确规定:"除非国内法已提供了适当的保护措施,禁止

[30] [日]大岛明:"个人信息保护法制的完善与地方癌症登记事业",载地方癌症登记协议会:《时事通讯》2003年8月第13号。

对揭示以下内容的个人数据进行自动化处理:人种、政治主张、宗教或其他信仰以及与健康或性生活有关的个人数据。与刑事判决有关的个人数据,也不应当被自动化处理。”

对敏感个人信息规定最为严格、详细的当数欧盟指令。欧盟指令第8条规定:

“1.各成员国应禁止处理显示种族或民族起源、政治观点、宗教或哲学信仰和工会资格的数据,并禁止对有关健康和有关性生活的数据进行处理。

2.第1款的规定不适用于下列情况:

(a)数据主体明确表示同意处理这些数据,除非成员国的法律规定数据主体的同意不能解除第1款的禁令;

(b)处理对于管理者在就业法范围内履行其义务和行使特殊的权利是必要的,但限于就足够的保护措施给予规定的国家法律的授权范围;

(c)如果数据主体在身体上或法律上无法表示同意,但是处理对于保护数据主体或其他人的重大利益是必要的;

(d)处理是在基金会、组织或其他非营利性机构出于政治、哲学、宗教或工会目的且有足够保障的活动中进行的,条件是该处理只涉及该机构的成员或与该机构签订有关其目的的例行合同的人,而且未得到数据主体的同意,不得向第三方公开这些数据;

(e)处理所涉及的数据明显是由数据主体所公开的或该处理对于提出、行使或保护合法要求是必要的。

3.第1款的规定不适用于下列情况:如果出于预防医学、医疗诊断、提供护理和治疗或保健服务管理的目的而提出对数据进行处理的要求;如果是在卫生专业部门在国家法律或国家管理机构制定的法规下,出于其专业保密的义务而进行的数据处理,或是其他人由于同样的保密义务而进行的处理。

4. 在遵守提供适当的保护的条件下,各成员国可以出于实际公共利益的原因,通过国家法律或监督机关的决议规定除第 2 款以外的免除情况。

5. 只有在官方机构的管理下,或者根据国家法律规定提供适当的特殊保护措施时才能处理涉及犯罪、宣判或安全措施的有关数据,成员国可以授予减损权,但必须根据国家规定提供适当的特殊保护措施。但是,宣判的完整登记只能在官方机构的管理下予以保存。

各成员国可以规定,涉及行政制裁或民事判决的数据也必须在官方机构的管理下进行处理。

6. 应向欧委会通知第 4 款和第 5 款规定的对第 1 款的减损情况。

7. 各成员国应该决定在何种条件下才可以对国家识别号码或任何其他通用的识别符进行处理。”

欧盟指令的规定不但影响了欧盟成员国的立法,对其他许多国家的个人信息保护立法也产生了重大的影响。例如,阿根廷个人数据保护法明确将敏感数据界定为“揭示个人人种和种族,政治观点、宗教的、哲学的或道德的信仰,工会会籍和有关健康状况或性嗜好或行为之数据”。同时,法律还规定:

“1. 禁止强迫个人提供敏感数据。

2. 敏感数据仅在存在法律所准许的普遍利益的情况下或在为统计或科研目的且不能识别数据所有者的情况下才可以被收集和处理。

3. 禁止建立所存储信息直接或间接揭示敏感数据的文件、数据库、登记簿。在不违反前述规定的情况下,天主教堂,宗教协会和政治、工会组织可被授权对其成员进行数据登记。

4. 有关犯罪或其他违法记录的数据只能由公共权力机构在相应的法律和法规规定的框架内进行处理。”

尽管在个人信息保护法律中规定敏感个人信息的国

家与地区越来越普遍,但是,仍然有相当数量的国家或地区没有做类似的规定。例如,经合组织指南、APEC 协议中的隐私保护原则,日本、韩国与我国台湾地区就都没有明确规定敏感个人信息。经合组织并且专门在其解释性备忘录中对此进行了说明:"有人可能主张说,列举本质上敏感的数据种类和范畴既是可能的,也是必须的,对此种数据的收集应当受到限制甚或是禁止。在欧洲的立法中存在类似的先例(例如,种族、宗教信仰、犯罪记录)。另一方面,也可以认为,任何数据本质上都不是'私人的'或'敏感的',但是,它们可能在特定的语境下和在被放置到不同的用途中时变成'私人的'或'敏感的'。例如,这种观点反映在美国的隐私立法中。专家团讨论了许多敏感标准,如差别待遇的风险,但是,它并不认为,给那些通常被认为是敏感的数据下定义是可能的。因此,第七段仅包含一个应当限制个人数据收集的普遍阐述。"

对于这个问题,在起草专家建议稿过程中,进行了仔细的研究和分析。我们认为,尽管在我国确实有必要加强对某些敏感个人信息的保护(如传染病病人、艾滋病患者),但是,在个人信息保护法中不宜采用敏感个人信息概念。理由在于:(1)域外立法中的敏感信息概念含义非常广泛,包括了政治权利、宗教信仰、结社自由、健康、性生活与司法公正等许多方面。在我国,由于国情的不同(我国宪法中明确规定了党的领导原则和坚持马列主义、毛泽东思想、邓小平理论与"三个代表"重要思想),如果采用含义广泛的敏感个人信息概念,会导致个人信息保护法与我国宪法和根本政治制度的冲突。如果另起炉灶,采用含义狭窄的敏感个人信息概念(如集中于个人健康信息),一来没有必要,可以直接使用相关的概念;二来容易授人以柄,在国际人权对话中陷于被动。(2)对于我国实际生活中各个方面收集个人信息过多,甚至收集直接涉及类似个人健康、医疗信息的问题,完全可以通过单行立法的方式

解决,没有必要一定要在个人信息保护法中规定敏感个人信息。实际上,近年来有关方面已经制定了不少类似的规定(见上文对我国个人信息保护法律现状的说明),专家建议稿也明确规定了对个人信息的保护模式采取综合立法、特别立法、自律与技术保护相结合的形式,并不排除另行制定特别法。(3)不采用敏感个人信息概念,在域外立法当中也是一种比较常见的选择。在可以预见的未来,这种选择都是合理的,会为相当数量的国家或地区所支持,不会在国际舞台上陷于孤单或被动。

第十四,关于法律的执行机构问题

在国际社会,为保证个人信息保护法的顺利实施,各国均对法律的执行机构给予了高度的关注。根据欧盟指令第 28 条的规定,其成员国应当设立一个或多个专门的机构负责独立地监督个人信息保护法的实施,凡制定的法律、法规中涉及个人信息的,有关部门应当咨询该机构的意见;同时,该机构享有相应的调查权、依照职权或者依照有关当事人的申请而对相应的违法行为进行查处的权力以及通过介入诉讼维护法律实施的权力等。根据欧盟指令第 18 条的规定,个人信息处理者进行全部或部分处理操作或为了单一或几个相关目的而进行整套操作之前,必须通知执行机构。

根据欧盟指令的规定,采用欧洲立法模式的国家均设立了相应的执行机构。例如,在丹麦,依照《个人数据处理法》的规定,设立了信息保护局,负责独立执法。与之相配套的便是登记制度和监督制度。处理个人信息的机构在处理各种有通知义务的个人信息之前,均须向该信息保护局通报包括信息处理者的情况、处理的种类和目的、信息

主体的种类和信息的种类、数据的接收者、信息的安全管理措施等事项,并应得到信息管理局的授权。信息保护局有权主动或者按照信息主体的投诉对各种信息处理行为进行监督检查,可以无须法院令状而进入信息处理者办公场所进行检查,可以命令信息处理者采取停止处理、删除、修改等措施以保护个人信息。在法国,国家信息处理与自由保护委员会为主管机构,公共部门进行信息处理前应征求其意见(法国 1978 年《数据保护法》第 15 条),非公共部门仅须向其登记备案即可,以便于进行事后管理(第 16 条)。在阿根廷,根据《个人数据保护法》的规定,在司法部设立了专门的委员会负责法律的实施。在澳大利亚和加拿大,都是由隐私专员办公室负责执行《隐私权法》。在救济机制上,英国还专门设立了信息保护审判所,对信息专员做出的各种行政决定所涉及的案件进行审理(英国《数据保护法》第 6 条)。客观地看,欧盟执行模式所采用的这种执行机构在个人信息保护方面拥有较大的权限,可以有效地实施个人信息的保护。

当然,对于欧盟指令所要求的这种执行模式,一直存在一些不同的看法。在经合组织指南中,就并未专门涉及执行机构问题。又比如,日本在制定个人信息保护法的过程中,就指出:如果像欧洲那样,设立对任何领域都拥有管理权限的个人信息保护机关,则有可能大幅度地限制非公共部门本应自由的活动,这不符合日本的国情,且与其行政改革和放宽管制的潮流相悖,所以应构建富有成效的事后救济体系;至于适用于所有领域的登记制度,则会限制各种非政府部门从事经济活动、增加其经营成本与行政管理成本。[31]因此,日本最终没有设立专门的管理机构,对于行政机关的个人信息处理,由该机关事前向总务大臣通报相关事项,对于独立行政法人、非公共部门的个人信息处理,则没有通报制度,分别由总务大臣要求独立行政法人、主管非公共部门的内阁大臣视情况要求该部门提交实施

[31] 参见日本高度信息化通信社会推进本部个人信息保护研讨会发表的"我国个人信息保护系统的存在方式(中间报告)",载《法律时报》(日本刊物)第 72 卷第 10 号。

个人信息保护法的报告。同时,2003 年出台的针对行政机关和针对独立行政法人的个人信息保护法均规定,凡与个人信息处理有关的行政复议案件,复议机关必须咨询专门设立的"信息公开与个人信息保护审查会"的意见。该机构的委员具有较高的独立性和专业性,虽不能直接做出复议决定,但习惯上,复议机关一般比较尊重其意见。对于非公共部门,主管大臣可以针对其违法或者不当的个人信息处理行为发出指南或者命令;同时,法律还允许设立各种民间团体参与处理纠纷。在韩国,行政自治部负责公共部门的个人信息保护,与之有关的各种争议通过一般的行政复议和行政诉讼程序解决(参见韩国《公共机关个人信息保护法》第 6、15、21 条),而信息通信部则负责非公共部门的个人信息保护;同时,设立了"个人信息保护纠纷调停委员会"负责对纠纷进行调解(参见韩国《关于促进利用信息通信网与保护信息的法律》第 4 条及第 4 章)。

法律的执行机构问题,在我国是一个决定性的问题。我国至今都没有专门的政府信息资源主管部门,这必然会影响到法律的制定和实施。为此,专家建议稿专门对政府信息资源主管部门的职责做了明确的规定,以推动形成有效的法律执行机制。考虑到我国政府机构的现状,专家建议稿对实施本法的主管部门并没有统一的要求,它既可以是专门设立的信息资源管理机构,也可以是内设有专门机构或人员的一般办事机构,如政府办公厅或秘书局。从政府信息化的长期发展和国外的经验考虑,我们认为,该机构最好是专门设立的信息资源管理机构,而且其职责应该相对比较明确和跨部门,全面负责政府信息资源管理与信息技术利用方面的工作。可以设想对我国目前的政府机构进行一定的重组或改革,在现有的部门的基础上构建一个综合性的政府信息资源主管部门。

为体现执法机构的独立性、专业性和权威性,借鉴国外专门设立信息专员或独立委员会的经验,专家建议稿同

时规定:“有条件的地方,政府信息资源主管部门可以吸收本部门之外的专家,组建独立的信息委员会,受理行政复议申请,做出行政复议决定,行使其他行政管理权力。”这一规定既考虑了我国的现状,也顾及制度未来发展的需要,各地可以根据实际情况,做出多种不同的制度安排或选择。

第十五,关于行业自律机制问题

隐私权是一种非常容易受到侵犯的权利,某些个人信息(如个人健康信息)一旦公开或泄露,后果就无法再挽回。另一方面,为了保证社会的信息自由流动,又必须让政府机关或其他个人信息处理者进行必需的个人信息处理。因此,处于政府与单个信息处理者之间的行业自律机制就具有了特别的意义。没有行业自律机制,仅仅依靠政府规制,要么会造成高昂的执法社会成本问题,要么不可能达到保护个人信息的目的。正因为如此,不论是美国立法模式还是欧盟立法模式,均对行业自律机制给予了充分的肯定。例如,欧盟指令第27条规定,各成员国与欧盟委员会应根据不同行业的特点,鼓励业界制定实施指令与成员国法律的行为准则。成员国应该为行业协会或代表处理者的其他组织制定规定,使其能够将起草的行为准则送交国内执法机构征询意见。如果执法机构认为行为准则符合指令的规定,应该征求数据主体或其代表的意见。经合组织指南第19条也规定,不论是以行为准则的形式还是以其他的形式,成员国应鼓励和支持自律机制。当然,即使在发达国家,要使行业自律机制真正能够在保护个人权利中发挥作用,还有很长一段路要走。[32]

在我国,行业自律机制(尤其是传统的行业协会)面

[32] 行业自律机制在实践中存在诸如不愿意对违反章程的组织成员采取措施以及更多考虑的是信息处理者而不是消费者的利益的问题。参见,Just How Trusty is Truste, *Wired*, April 9, 2002, http://www.wired.com/news/exec/0,1370,51624,00.html。

临的各种问题就更多了,更需要长时间在实践中逐步培育。综合考虑了域外立法的经验和我国的实际,专家建议稿专门以一节对行业自律机制做了规定。这种安排的考虑在于:(1)行业自律机制是个人信息保护制度中不可缺少的一个环节,尽管其作用的发挥需要许多外部条件的支撑。(2)法律中规定的内容详细一些,有利于在实践中进行各种形式的探索,也有利于传递政府职能转变的信号。(3)这种规定并不改变我国对行业协会的现行管理制度。协会的成立仍需要履行相应的法律程序,政府信息资源主管部门只是在协会成立以后,对其业务工作进行指导和监督。并且,行业自律机制要真正发挥作用,还必须在政府机关与协会之间形成良性互动。(4)行业自律组织在个人信息处理领域能够承担的责任非常广泛,可以根据实际情况逐步试点、推开。

第十六,关于信息主体的权利

个人信息权利意味着个人对于与自己有关的各种信息进行收集、储存、传播、修改等所享有的决定权和控制权。另一方面,个人作为社会的一分子,肯定会被他人"所视"或"所知"。每个人都不能以自己的信息控制权,剥夺他人"视"或"知"的权利。因此,需要在个人信息保护法中,明确信息主体权利的边界,使其能够控制自己的信息不被滥用;同时,也保证社会"知"的权利能够正常行使。

信息主体的权利分别涉及个人信息处理的三个主要环节,即信息的收集、信息的使用和信息主体获得与自己有关信息的权利。域外立法在最后一个环节上差别不大(尤其是均授权信息主体可以自政府机关获得与自己有关的信息的权利),但在前面两个环节上则存在不同的选择。

有些立法更多偏向信息主体的控制权,有些则更多地偏向社会"知"的权利。从域外立法的相关规定看,信息主体主要享有如下权利:

(1)决定是否提供本人的个人信息的权利。在信息处理者处理个人信息的行为面前,信息主体不是完全被动的,可以根据信息处理者的业务范围、收集目的等决定是否向其提供本人的个人信息。事实上,各国的政府信息公开法均在一定程度上涉及了这一问题,即,一般而言,凡被请求公开的政府信息中涉及第三人的个人信息的,被请求公开的政府机关有义务征询该第三人的意见,第三人还可以对政府机关无视其意见公开其个人信息的行为提起反信息公开诉讼。但是,信息交流与共享是社会发展和个人发展所必需的,因此,个人信息绝不可能完全依照信息主体的意见予以保密,许多情况下,个人信息的收集是在无法取得信息主体的同意,甚至是在其毫不知情的状况下进行的,比如个人信用信息、重要医疗信息等的收集。而且,某些情况下,为了促进信息共享,只要符合最初的收集目的并采取妥善的安全保障措施,未经本人同意而转让一部分个人信息也是被允许的,例如行政机关为履行其职责而可以自其他机关处获得某些个人信息。

(2)请求信息处理者告知个人信息的利用目的等事项的权利。个人信息处理者直接或者间接向信息主体收集个人信息的,应当在收集之时或者之后某一合理的时间内向信息主体告知包括个人信息处理者的基本情况、个人信息的收集利用目的、信息来源等的相关事项,这是信息主体行使个人信息控制权的前提。但是,如果告知这些事项(尤其是利用目的)将有可能危及本人或者第三人的生命财产安全、个人信息处理者的正当权益或者国家安全、社会公共利益的,本项权利将受到限制(比如丹麦《个人数据处理法》第28、29、30条,日本《个人信息保护法》第19条)。

(3)请求个人信息处理者告知是否拥有本人的个人信息,并公开该个人信息的权利。随着社会的不断发展,越来越多的公共部门和非公共部门在收集、保存、交换着大量的个人信息,这些信息处理有许多是在信息主体不知情的情况下进行的,而且,这些信息往往对个人的就业、融资、享受各种公共服务、人身与财产安全等有着重要的影响。从保护个人的合法权益的角度讲,信息主体必须享有要求个人信息处理者告知它是否拥有其个人信息以及拥有哪些个人信息的权利,并可以要求个人信息处理者向其公开与之有关的个人信息。

(4)请求订正、删除或者停止使用有关个人信息的权利。与前一项权利相关联,信息主体发现个人信息处理者所处理的本人的个人信息与事实不符的,有权利要求其依照事实予以订正、删除或者停止使用。这是防止有关的个人信息处理者依照与事实不符的个人信息而对信息主体做出错误决定的保障(比如冰岛《处理个人数据中保护个人法》第25条、日本《个人信息保护法》第26条等)。另外,如果处理个人信息的合法理由已经不存在、未经本人同意或者以其他不正当手段处理个人信息的,信息主体也可以请求个人信息处理者删除或者停止利用该个人信息(比如冰岛《处理个人数据中保护个人法》第26条、日本《个人信息保护法》第27条等)。

(5)获得救济的权利。没有救济就没有权利。上述各项具体权利受到侵害的,信息主体可以采取向个人信息处理者投诉、要求个人信息处理的主管部门予以查处的方式或者通过诉讼途径予以解决。个人信息处理者为公共部门的,则主要是通过行政复议、行政诉讼等途径解决,个人信息处理者为非公共部门的,则主要是通过民事诉讼予以解决。

专家建议稿对信息主体的权利给予了高度的关注,并体现了如下几个方面的立法意图:(1)整部法律均体现了

以信息主体的个人权利来制约违法信息处理的基本思路，以减少执法层次，提高个人权利的保护效率。(2)信息主体获得个人信息的权利(包括要求更正与停止使用的权利)是整部法律的重点，意图在于以最为严格的措施来防止个人信息的被滥用，满足信息主体的知情权与参与权。(3)在个人信息的收集与使用环节，主要由法律划出明确的界限，使政府机关与其他个人信息处理者知道应该如何行为；同时，明确规定公开透明的查询机制，通过公开机制来制约违法的个人信息收集与使用。当然，在这两个环节，也授予信息主体一定的控制权，以减少不必要的信息收集与使用。(4)全面设计了可行的救济制度，使信息主体的权利能够得到切实的保障。(5)在法律原则部分明确规定信息主体行使其权利不得妨碍他人的权利与自由，不得损害国家利益与社会公共利益，在制度设计上尽量体现信息主体的权利与其他合法权益之间的平衡，保证信息的自由流动。

第十七，关于跨境信息流问题

对跨境信息流加以规范，是欧盟指令的一个重要方面。根据《欧盟指令》第25条的规定："各成员国应该在立法中规定，只有当第三国确保能够提供充分的保护时，才能向其转让正在处理或在转让后将要被处理的个人数据。判断第三国是否提供了充分的保护，需要考虑的因素包括数据的性质、协议中的处理的性质和持续时间、始发国和目的国、第三国一般法与特别法的法律规定、职业规范以及安全措施。一旦欧盟委员会认定第三国未达到充分保护的水平，成员国会采取措施阻止向第三国传输个人数据。欧盟委员会既可以根据第三国的国内法，也可以根

据与第三国签署的国际协议,认定其是否已经达到充分的保护水平。一旦欧盟委员会做出决定,成员国必须采取相应的措施。目前,欧盟认定其国内法已经达到充分保护水平的国家只有加拿大、阿根廷、匈牙利与瑞士,同时,欧盟委员会正在对包括新西兰、澳大利亚和中国香港的隐私保护体制进行审议。根据国际(安全港)协议认定满足充分保护要求的只有美国。

《欧盟指令》第26条同时也规定了达不到充分保护水平仍可以进行个人数据传输的两种例外情况:一是法定例外,二是合同例外。

法定例外的情况包括:(1)数据主体明确同意协议中的传输;(2)传输对于履行数据主体与处理者所签合约或者根据数据主体提出的要求采取的预约措施是必要的;(3)传输对于处理者为了数据主体的利益与第三方签订或履行合同是必要的;(4)传输对于重要的公共利益是必须的或者法定的,或者为了法律诉求的提出、实施或抗辩是必须的;(5)传输对于保护数据主体的重要利益是必要的;(6)传输来自于根据法律或规章、规定要向公众提供的信息,记载于一般公众或证明有合法利益的任何人只要符合条件都可以公开查询的登记簿。

合同例外是指如果处理者可以根据合同条款,得到对方保护个人隐私和基本权利的充分担保,则成员国可以授权进行个人数据传输。为此,欧盟制定了许多包含标准数据保护条款的格式合同。这种格式合同要求数据处理者尊重通知、统一或区域法律救济等数据处理原则。2001年7月,欧盟委员会发布了最终的标准合同条款。在标准合同条款的起草过程中,美国对其进行了批评,指责它"过于烦琐"并且"与现实世界的运作不符"。

无论对欧盟指令中跨境信息流的规定评价如何,[33]一个不容回避的事实是,欧盟的规定使跨境个人信息传输成为了一个国际问题,也使欧盟之外的其他许多国家在立法

[33] 例如,《经合组织指南》(第17条、第18条)与《欧洲理事会协定》(第12条第2款)均强调了各国不得立法限制个人数据跨境流动的原则。

中纷纷效仿。可以预见,未来的国际贸易纠纷,将会与个人信息保护有关。个人信息保护,甚至完全有可能被当做某种新形式的贸易壁垒。为此,专家建议稿专门对这个问题做出了一条规定。做这种规定的主要考虑是:(1)可以维护国家利益,防止关系国家安全或国际法义务的某些个人信息进行跨境传输。(2)由于不能排除有些国家未来可能会对我国采取限制信息传输的措施,法律中做出专门的规定可以为采取对等措施提供法律依据。(3)授予国务院政府信息资源主管部门一定的权力,使其可以根据实践的进一步需要,制定一套完备的认定国外保护水平的制度。(4)与其他国家的通行做法保持一致。

第十八,关于刑事责任问题

从其他国家与地区个人信息保护法立法与执法的情况看,对违反个人信息保护法的行为追究刑事责任是普遍的做法。否则,对个人信息权利的保护就只会停留在字面上。例如,《欧盟指令》第24条规定,各成员国应采取适当的措施以确保指令的全面实施,特别应该制裁违反指令实施的行为。奥地利《个人数据保护法》第51条第1款规定:"无论何人,如果使用已经被委任的,或者由于专业原因而获得的个人数据,或者非法获取数据,并为个人使用或者把这些数据提供给他人或者为营利或致害目的而公开这些数据,除去数据所有人应受保护的利益以外,应该由法院处以一年的监禁处罚,除非另外的条款规定了更重的惩罚。"冰岛《处理个人数据中保护个人法》第42节规定:"根据设定刑事制裁的其他法律,违反本法或其他依据本法制定的行政法规的个人都应当被处以罚款或最高刑为三年的监禁。如果个人数据保护局发布的命令没有被

遵守,则应当对违法者施以同样的处罚。”

波兰《个人数据保护法》对各种违反法律规定的行为设定了各种不同的刑事责任。第49条规定:“1.如果进行处理的个人数据,是取自禁止进行处理的、或者是并未授权行为人进行相关数据处理的数据文件系统中,行为人将被处以罚款、部分限制自由或者最高两年的监禁。2.违反本条第1款进行的数据处理行为,如果还涉及种族、人种、政治观点,参加的宗教派别、政党、商业团体,以及涉及健康状况、遗传基因、嗜瘾或者性生活的相关信息,行为人将被处以罚款、部分限制自由或者最高三年的监禁。”第50条规定:“作为数据文件系统的管理员,如果保存的个人数据与建立系统之目的不相符合,行为人将被处以罚款、部分限制自由或者最高一年的监禁。”第51条规定:“1.作为数据文件系统的管理员或者有义务保护个人数据的人员,向未经授权的人公开或者提供访问权限的,行为人将被处以罚款、部分限制自由或者最高两年的监禁。2.如果是出于过失,实施上一款规定之行为的,行为人将被处以罚款、部分限制自由或者最高一年的监禁。”第52条规定:“作为数据文件系统的管理员,无论基于故意或者是过失,违犯保护个人数据免于未经授权的转移、损害或者破坏的义务的,行为人将被处以罚款、部分限制自由或者最高一年的监禁。”第53条规定:“未能履行登记数据文件系统义务的,行为人将被处以罚款、部分限制自由或者最高一年的监禁。”第54条规定:“管理员未能告知与数据相关的当事人,其享有的权利或者可以依照本法受益的相关信息的,行为人将被处以罚款、部分限制自由或者最高一年的监禁。”

在我国,有法不依,执法不严,以罚代刑等是非常常见的现象。尤其是因为个人信息保护在我国属于一个新领域,普通公众与专业信息处理人员的法律意识都还需要加强。在这种背景下,如果对于违反个人信息保护法的行为

没有刑事制裁措施,仅仅靠普通的民事救济机制或者行政处罚措施,法律的实施效果是很难保障的。为此,专家建议稿在法律责任部分反复提到了刑事制裁。当然,鉴于我国刑法的立法结构,单行法律无法直接规定罪名和刑罚,因此,刑事责任的规定都是采用的交叉索引方式。要追究刑事责任,必须根据刑法的罪名和制裁幅度执行。

我国刑法中并没有直接规定侵犯个人信息权利的刑事责任。因此,要实施刑事制裁,必须从相关的刑法规定中找到依据。例如,对政府信息资源主管部门工作人员追究刑事责任,可以适用刑法有关职务犯罪的规定,如贪污贿赂罪、渎职罪。如果政府机关工作人员在诉讼程序中销毁、篡改作为证据的政府信息,可能会构成《刑法》第306条所规定的毁灭证据、伪造证据罪或者《刑法》第307条所规定的帮助毁灭、伪造证据罪;故意不向信息主体公开政府信息或者阻碍公开政府信息,可能构成《刑法》第397条所规定的滥用职权罪。对其他个人信息处理者追究刑事责任,也要根据行为的性质,分别适用不同的条文。例如,许多情况下可以适用《刑法》第286条的规定:"违反国家规定,对计算机信息系统功能进行删除、修改、增加、干扰,造成计算机信息系统不能正常运行,后果严重的,处五年以下有期徒刑或者拘役;后果特别严重的,处五年以上有期徒刑。违反国家规定,对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作,后果严重的,依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序,影响计算机系统正常运行,后果严重的,依照第1款的规定处罚。"

为使个人信息保护法能够顺利实施,也为了体现刑法的权威性和公正性,我们认为,个人信息保护法通过以后,时机合适时,应由最高人民法院通过司法解释的形式,对法律中涉及刑事责任的几个条文,进一步予以明确。

第十九,关于"9·11"以后国际社会个人信息保护政策的变化趋势问题

"9·11"改变了世界,也对个人信息保护制度产生了多方面的影响。

"9·11"之后,联合国通过了1368号决议,呼吁加强国际合作,防止和打击恐怖主义;北约援引条约第5条,宣称向任何一个北约成员的攻击等于是向所有北约国家的攻击;欧洲理事会谴责了攻击并呼吁加强在犯罪问题上的国际合作,后来,欧洲理事会召开大会呼吁成员国批准打击恐怖主义公约,取消对公约的任何保留,将警察的权力扩大到"恐怖主义资讯及其破译";欧盟也力推欧盟逮捕令、反恐共同立法框架、加强情报与警察合作、冻结恐怖组织财产以及制定反洗钱指令;经合组织坚决支持打击金融洗钱行动计划,并与发达国家七国集团和欧盟委员会一道,呼吁加强打击恐怖融资活动。这些国际合作的呼吁被视为各国立法的前哨。

为对付恐怖主义,截至2002年9月,据美国OMB统计,联邦政府机构已经制定了58个新规章。到2003年3月,据美国审计办公室统计,美国已经有九份新的国家战略出台。美国联邦与州政府通过了无数的法律。美国通过的《爱国者法》,加强了政府的监控权,减少了监督与正当程序的要求。政府机关内部,政府机关之间以及政府机关与私营部门的信息共享得到了加强。为某一目的收集的数据可以为其他目的使用和共享。美国《爱国者法》增加了FBI与CIA之间的信息共享,并增加联邦执法部门与地方执法部门之间的信息共享。

2001年10月,布什总统致信欧盟委员会主席,要求欧盟"在执法和反恐需要的背景下考虑数据保护问题",

"修改要求强制销毁数据的隐私指令草案,允许在合理的时间内截留关键的数据"。美国司法部向欧盟打击网络犯罪工作组提出了几份建议,提出"任何数据保护制度都必须在保护个人隐私,满足服务提供商保证其网络安全和防止欺诈的合法需要以及维护公共安全三者之间维持平衡"。2002 年 5 月,发达国家八国集团司法部长与内政部长会议再次要求各国,"保证数据保护立法实施中考虑公共安全与其他社会价值,尤其是应该允许截留和保存对网络安全、执法调查或公诉重要的数据,考虑因特网与其他正出现的各种技术"。

除美国之外,澳大利亚在反恐立法方面最为突出。2002 年,澳大利亚国会审议了至少八部反恐法案。加拿大 2001 年 12 月制定反恐法,允许无证预防性逮捕和调查性听证。巴厘岛爆炸案后,印尼政府授权执法部门可以无须证据拘留个人。这一权力在 2003 年 3 月正式规定到法律中,可以根据初步证据拘留个人达六个月。2001 年 12 月,英国通过反恐法律,授权中央政府一个部门可以最长七年截留通信数据。英国与加拿大并且准备制定法律,使执法部门可以获得旅行者的信息,然后将这些信息与其他个人信息进行比对,用于包括反恐在内的多个目的。法国扩大了警察无证搜查私有财产的权力。德国对截查通信减少了授权限制并增加了执法部门与国家安全部门的数据共享。澳大利亚与加拿大都通过立法重新定义恐怖主义活动,如果怀疑有恐怖主义活动或恐怖主义分支组织,授权国家安全机关为内政目的行使监控权力。印度通过法律,允许当局未经审判拘留嫌疑犯、加强监听和扣押资金与财产。

与此同时,在许多国家,信息主体的知情权受到了很大的限制。为保护敏感的调查和情报数据,一些数据库被从数据保护法和信息自由法中的执行中豁免。

在这种转变过程中,作为个人信息保护先驱的欧盟也

发生了许多变化。

1997 年,欧盟制定了电信隐私指令,以补充 1995 年指令。电信隐私指令对电话、数字电视、移动网络与其他电信系统提供了特别保护,要求运营商与服务提供商承担诸多义务,以保证使用者通信的隐私。2000 年 7 月,欧盟委员会提出在电子通信领域制定新的隐私指令的建议,该建议是欧盟在电子通信市场加强竞争"一揽子"指令的一部分。最初,建议的新的指令应该是加强对个人隐私权利的保护,但是,在讨论过程中,欧盟部长理事会开始推动加入截留数据条款,要求互联网服务提供商与电信运营商为执法目的,储存所有电话、电子邮件、传真与互联网活动的信息。这些建议遭到欧盟议会大部分议员的反对。

"9·11"之后,政治环境发生了改变,欧洲议会面临着来自各成员国的巨大压力。最终,2002 年 5 月 30 日,欧洲议会通过了欧盟部长理事会支持的新的隐私指令,6 月 25 日,欧盟部长理事会予以通过。根据新的指令,成员国现在可以通过法律,强制要求截留所有通过移动电话、短信、固定电话、传真、电子邮件、聊天室、因特网或者任何其他电子通信装置传送的信息。这种要求可以为国家安全及预防、调查与追究犯罪等目的而提出。

在美国与欧盟的互动方面,美国根据 2001 年民航与运输安全法的规定,与欧盟就传送民航乘客个人数据问题进行了长时间的谈判。欧盟负责个人数据保护的工作组虽然注意到了协议中的信息共享的一些问题,[34]最终双方还是于 2004 年 5 月签署了航空安全条约。

我们认为,对于"9·11"之后各国所采取的措施和已经发生和正在发生的变化,必须要有全面、清醒和客观的认识。这种认识直接决定着我们是否应该制定法律,以及如果制定法律应该如何进行具体的制度设计这样一些根本性的问题。

对于国际社会的变化,根据目前观察可以得出的几点

34 Article 29 Data Protection Working Party, Opnion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, 11070/03/EN, Adopted on 13 June 2003.

结论是:(1)这种变化有必然性和长期性,是时代特点的反映。并且,在可以预见的未来,反恐与国家安全都会继续主导许多国家的立法。这种变化说明,个人信息保护必须与其他利益平衡。即使没有"9·11"事件,个人信息保护立法同样需要平衡不同的利益。因此,立法不能只顾及某一个方面的利益而忽略了其他同样重要的利益。(2)这种变化从本质上看都是在各国现行宪政和法治框架内进行的,从根本上说并没有颠覆各国的个人信息保护制度。如果说有什么变化,那就是在平衡上,国家安全的考虑占据了更多的分量。并且,个人信息保护问题在反恐的形势下同样也显得更为突出。对于一些国家"9·11"之后过度干涉个人隐私的举措,许多国家的民间组织、新闻界、学术界乃至议会,都开始发出越来越多的不同声音。[35]这种情况表明,即使在反恐的环境下,也不能走到另一个极端,忽视对个人权利的保护。在这个问题上,各国实际上已经积累了许多有益的经验。[36](3)面临反恐的新形势,个人信息保护法要平衡个人权利与其他社会利益,操作难度更大,对立法的要求更高。(4)专家建议稿已经充分考虑到了"9·11"事件的影响,因此,立法建议稿中已经对国家安全与个人权利的协调给予了充分的考虑,进行了相应的制度设计,不会出现因为个人信息保护而影响国家安全的情况。(5)由于我国的大环境、民主法制水平等与发达国家相比存在明显的差别,因此,对"9·11"后某些发达国家的反应不能过于机械地片面解读,否则,不利于建设我国的政治文明和实现依法治国的战略目标。

[35] 美国爱国者法中日落条款规定的时间是2005年年底,目前美国国内对该法充满争议的措施是否应该延长有很多争议。反对爱国者法的运动颇具规模,超过一百个地方政府通过了地方法律反对爱国者法。available at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=11256&c=206.

[36] 在秘鲁,高等法院宣布藤森政府期间制定的反恐法令违宪,必须对1800人的判罚进行复审。

1998年,菲律宾最高法院裁决一项全国身份证立法违反了宪法规定的隐私权利。Philippine Supreme Court Decision of the National ID System, July 23, 1998, G.R. 127685, available at http://bknet.org/laws/nationalid.html. 1991年,匈牙利宪法法院裁决一部建立多重使用目的个人身份号码法律违反宪法规定的隐私权。Constitutional Court Decision No. 15-AB of 13 April 1991, available at http://www.privacy.org/pi/countries/hungary/hungarian_id_decision_1991.html.

1997年,修正后的葡萄牙宪法第35条第5款明确规定:"不得给公民发放多目的的全国性身份号码。" Constitutional Court Decision No. 15-AB of 13 April 1991, available at http://www.privacy.org/pi/countries/hungary/hungarian_id_decision_1991.html.

附录:域外个人信息保护法名录

FULU: YUWAIGERENXINXIBAOHUFAMINGLU

国家或地区名	(制定或)实施时间	名称	备注(英文名)
阿根廷	2000 年 11 月	个人数据保护法	Law for the protection of personal data
澳大利亚	1988 年	隐私法	Privacy Act
澳大利亚	2001 年 11 月	(私营部门)隐私修正法	Privacy Amendment (Private Sector) Act
奥地利	2000 年 1 月	数据保护法	Datenschutzgesetz 2000
比利时	1992 年制定,1998 年 12 月修正	数据保护法	Data Protection Act 1992 www. law. kuleuven. ac. be/icri/papers/legislation/privacy/engels
保加利亚	2002 年 1 月	个人数据保护法	Personal data protection act
加拿大	1982 年 2001 年	隐私法 个人信息保护与电子文件法	Privacy Act Personal information protection and electronic document Act (PIPEDA)
智利	1999 年 10 月	个人生活保护法	Law for the protection of private life (拉美第一个制定数据保护法的国家)

续表

国家或地区名	(制定或)实施时间	名称	备注(英文名)
捷克	2000 年 6 月	个人数据保护法	Personal data protection law (取代 1992 年的 Act on protection of personal data in information system)
丹麦	2000 年 7 月	个人数据处理法	Act on processing of personal data (取代 1978 年的私营部门登记簿法与公共权力部门登记簿法)
爱沙尼亚	1996 年 6 月	个人数据保护法	Personal data protection act
芬兰	1999 年 6 月	个人数据保护法	Personal data protection act (取代 1987 年个人数据档案法)
法国	1978 年	数据保护法	Data protection act (新法正在国民议会制定之中)
德国	1977 年	数据保护法	Data protection law (1994 年、1997 年分别修正,2001 年 5 月最终修正,以符合欧盟指令的要求) 德国黑森州于 1970 年制定了世界上第一部数据保护法

续表

国家或地区名	(制定或)实施时间	名称	备注(英文名)
希腊	1997 年	处理个人数据中保护个人法	The law on the protection of individuals with regard to the processing of personal data (Data protection act) 希腊是欧盟国家中最后一个制定数据保护法的国家
中国香港	1996 年	个人资料(隐私)条例	Personal data (privacy) ordinance
匈牙利	1992 年	个人数据保护与公共利益数据公开法	Protection of personal data and disclosure of data of public interest (个人数据保护法与信息公开法合一) www. osa. ceu. hu/yeast/AceessAndProtection/04. htm
冰岛	2000 年 1 月	处理个人数据中保护个人法	Act on the protection of individuals with regard to the processing of personal data (取代 1989 年个人数据登记与处理法) brunnur. stjr. is/interpro/tolvunefnd/tolvunefnd. nst/pages/1E685B166D04084D002569050056BF6F

续表

国家或地区名	(制定或)实施时间	名称	备注(英文名)
爱尔兰	1988 年	数据保护法	Data protection act
以色列	1981 年	隐私保护法	Protection of privacy law (1985 年修正)
意大利	1996 年	数据保护法	Data protection act Elj. strath. ac. uk/jilt/dp/material/1675-eng. htm
日本	2003 年	个人信息保护法 关于保护行政机关所持有之个人信息的法律 关于保护独立行政法人等所持有之个人信息的法律	
韩国	1994 年	公共机关个人信息保护法	Act on the protection of personal information maintained by public agencies
拉脱维亚	2000 年 3 月	个人数据保护法	Law on personal data protection 2002 年 5 月修正
立陶宛	1996 年	个人数据法律保护法	Law on legal protection of personal data 随后多次修正
卢森堡	1979 年	关于计算机处理中最少使用数据法	Act concerning the use of nominal data in computer processing

续表

国家或地区名	(制定或)实施时间	名称	备注(英文名)
荷兰	1988 年 2000 年	数据登记法 个人数据保护法	Data registration act 1988 Personal data protection act 2000 代替了上述法律
新西兰	1993 年	隐私权法	Privacy act
挪威	1978 年 2000 年	个人数据登记簿法	Personal data registers act 1978 Personal data registers act 2000 www. lovdata. no/all/hl-20000414-031. html
波兰	1997 年	个人数据保护法	Law on the protection of personal data protection
葡萄牙	1998 年	个人数据保护法	Act on the protection of personal data 代替 1991 Act on the protection of personal data with regard to automatic processing
俄罗斯	1995 年	俄罗斯联邦信息、信息化与信息保护法	Law of the Russia Federation on information, informatization, and information protection (law on information of personal character 在制定之中,它将使俄罗斯的个人数据保护与欧盟的要求更加一致)

续表

国家或地区名	(制定或)实施时间	名称	备注(英文名)
圣马力诺	1983 年	计算机个人数据收集、处理与使用法	Act on collection, elaboration and use of computerized personal data (1995 年修正)
斯洛伐克	1998 年	信息系统中个人数据保护法	Act on protection of personal data in information systems 代替 1992 年捷克斯洛伐克的同名法律
斯洛文尼亚	1999 年	个人数据保护法	Law on personal data protection (代替 1990 年的同名法律)2001 年 7 月再次修正
西班牙	1992 年	数据保护法	Data protection law 1999 年修正,与欧盟要求一致
瑞典	1998 年	个人数据法	Personal data Act 代替 1973 年的数据法(该法是世界上第一部国家层面数据保护法)
瑞士	1992 年	联邦数据保护法	Federal act of data protection
中国台湾地区	1995 年	“计算机处理个人数据保护法”	Computer processed personal data protection law www. virtual-asia. com/taiwan/bizpack/legalcodes/cpdpl. htm

续表

国家或地区名	(制定或)实施时间	名称	备注(英文名)
英国	1998 年	数据保护法	Data protection Act 代替 1984 年数据保护法
美国	1974 年	隐私权法	Privacy Act
阿尔巴尼亚	1999 年	个人数据保护法	
突尼斯	2004 年	数据保护法	非洲第一个专门的数据保护法
乌拉圭	2002 年	数据保护法	Habeas Data Law
亚美尼亚	2002 年	个人数据法	Law on Personal Data
巴西	1997 年	数据保护法	Law on Habeas Data
波黑	2001 年	个人数据保护法	
欧洲理事会	1981 年	有关个人数据自动化处理的个人保护协定	CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA
经济合作与发展组织	1980 年	关于隐私保护与个人数据跨疆界流动的指南	GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

续表

国家或地区名	(制定或)实施时间	名称	备注(英文名)
欧盟	1995 年	个人数据保护指令	Directive 95/ /EC of the European Parliament and of the Council On the protection of individuals with regard to the processing of personal data and on the free movement of such data

后记
HOUJI

2003 年年初,国务院信息办委托中国社会科学院法学研究所个人数据保护法研究课题组承担《个人数据保护法》比较研究课题及草拟一份专家建议稿,由我担任课题组负责人。课题组成员经过近两年的工作,分别形成了中期与最终研究报告。

本书是在上述研究的基础上形成的,但是,它纯粹是作者的个人观点,并不代表课题委托单位或作者供职单位的任何立场。中国社会科学院法学研究所吕艳滨博士,中国社会科学院研究生院温珍奎博士与翟小波博士对专家建议稿提出了宝贵的修改意见。吕艳滨博士与中国社会科学院研究生院陈世知同学参与了立法研究报告的资料收集和部分写作工作。

研究过程中,得到国务院信息办秦海先生与欧阳武先生的指导与大力支持。

美国商务部副助理部长 Michello O'Neil 女士与 IBM 中国有限公司政府事务部周梅月女士热心地为课题研究提供了部分资料,特此感谢。

2005 年 1 月 12 日
2006 年 7 月 8 日再修改

[General Information]
书名=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
作者=周汉华著
页数=104
出版社=北京市：法律出版社
出版日期=2006
SS号=11772780
DX号=000006113386
URL=http://book.szdnet.org.cn/bookDetail.jsp?dxNumber=000006113386&d=579DACB65744E5671A2B782BCB0EB04B